JP00/02041

30.03.00

EKU

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ３月３０日

出 願 番 号
Application Number: 平成１１年特許願第０８８３４６号

出 願 人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 １月２８日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３００１０４０

【書類名】　特許願

【整理番号】　9900210504

【提出日】　平成11年 3月30日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石黒　隆二

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　河上　達

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　田辺　充

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　江面　裕一

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　河原　博和

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、情報処理システム、並びに提供媒体

【特許請求の範囲】

【請求項１】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段と

を含むことを特徴とする情報処理装置。

【請求項２】　前記プログラムは、インタープリタに実行させるソースプログラムである

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記プログラムは、オブジェクトプログラムである

ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項５】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前

記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項６】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置、および認証局からなる情報処理システムにおいて、

前記情報処理装置は、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段と

を含み、

前記認証局は、

前記半導体ＩＣに実行させる前記プログラムを受信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、

前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段と

含むことを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、情報処理システム、並びに提供媒体に関し、特に、所定のデータを記憶し、所定の処理を行う情報処理装置および方法、

情報処理システム、並びに提供媒体に関する。

【０００２】

【従来の技術】

最近、CD（Compact Disk）、MD（Mini Disk）といった音楽データをデジタル式に記録または再生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

【０００３】

例えば、コピー元を制御するソフトウエアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

【０００４】

また、コピー元のソフトウエアに所定のハードウエアに記憶されているIDを利用して、コピー先の装置と相互認証させることも提案されている。

【０００５】

さらにまた、認証、暗号、および復号処理を、ワイアードロジックのハードウエアで実行させることも提案されている。

【０００６】

【発明が解決しようとする課題】

しかしながら、ソフトウエアだけで認証処理、暗号化処理、および復号処理を行うようにする場合、ソフトウエアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

【０００７】

また、所定のIDをハードウエアに記憶させ、パーソナルコンピュータ上のソフトウエアにより、これを読み出し、利用させるようにする場合、読み出されたIDがソフトウエアに転送される途中において読み取られ、解析、改竄されてしまう

恐れがあった。

【０００８】

さらに、認証処理、暗号化処理、および復号処理をワイアードロジックのハードウエアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理、および復号処理を行うようにするには、既存のハードウエアを新たなハードウエアと交換するか、新たなハードウエアを追加する必要が生じる。

【０００９】

本発明はこのような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

【００１０】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、半導体ＩＣに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信手段と、認証局から受信した、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体ＩＣに送信する送信手段とを含むことを特徴とする。

【００１１】

請求項４に記載の情報処理方法は、半導体ＩＣに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信ステップと、認証局から受信した、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ＩＣに送信する送信ステップとを含むことを特徴とする情報処理方法。

【００１２】

請求項５に記載の提供媒体は、情報処理装置に、半導体ＩＣに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信ステップと、認証局から受信した、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ＩＣに送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプ

ログラムを提供することを特徴とする。

【００１３】

請求項６に記載の情報処理システムは、情報処理装置が、半導体ＩＣに実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する通信手段と、認証局から受信した、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体ＩＣに送信する送信手段とを含み、認証局が、半導体ＩＣに実行させるプログラムを受信するとともに、情報処理装置に暗号化されたプログラムを送信する通信手段と、通信手段が受信したプログラムを所定の方式で暗号化する暗号化手段と含むことを特徴とする。

【００１４】

請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載の提供媒体においては、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信される。

【００１５】

請求項６に記載の情報処理システムにおいては、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信され、半導体ＩＣに実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化される。

【００１６】

【発明の実施の形態】

図１は、本発明を適用したネットワークシステムの構成例を表している。パーソナルコンピュータ１は、各種の処理を実行するCPU（Central Processing Unit）１２、各種のプログラムやデータを一時的に記憶するメモリ１３、並びに、各種のプログラムやデータを大量に蓄積するハードディスク１５を備えている。CD

-ROM (Read Only Memory) ドライブ１４は、装着されたCD-ROMに記録されているプログラムやデータを読み出す。IEC (Internationl Electrotechnical Commission) ６０９５８端子１６ａを有する音声入出力インタフェース１６は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。インターネット接続インタフェース１１は、インターネット４との間のインタフェース処理を実行する。インタフェース１７は、アダプタ３またはメモリスティックウォークマン２との間のインタフェース処理、並びに、入力部２およびディスプレイ３に対するインタフェース処理を実行する。

【００１７】

半導体ICとして、一体的に形成され、パーソナルコンピュータ１に装着されるアダプタ３のCPU３２は、インタフェース３１を介してパーソナルコンピュータ１のCPU１２と共働し、各種の処理を実行する。RAM３３は、CPU３２が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ３４は、パーソナルコンピュータ１の電源がオフされた後も保持する必要があるデータを記憶する。ROM３６には、パーソナルコンピュータ１から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) ３５は、計時動作を実行し、時刻情報を提供する。

【００１８】

メモリスティックウォークマン２は、不揮発性メモリ２３を有し、パーソナルコンピュータ１からインタフェース２１と認証装置２２を介して提供されたデジタル音楽データを記憶する。認証装置２２は、パーソナルコンピュータ１と不揮発性メモリ２３との間でデータを授受するとき、相互に認証処理を実行する。インタフェース２１は、パーソナルコンピュータ１との間のインタフェース処理、あるいは不揮発性メモリ２３に記憶されている音楽データを読み出し、ヘッドホンなどを介してユーザに提供するためのインタフェース処理を実行する。

【００１９】

パーソナルコンピュータ１は、インターネット４を介してEMD (Electrical Music Distribution) サーバ５と接続されており、EMDサーバ５から音楽データの

提供を受けることができる。

【００２０】

次に、図２のフローチャートを参照して、CD-ROMドライブ１４に装着されたCDから再生した音楽データをハードディスク１５に転送し、コピーする場合の処理について説明する。ユーザが入力部２を操作して、インタフェース１７を介してCPU１２に対してCD-ROMドライブ１４に装着されたCD（図示せず）から再生された音楽データをハードディスク１５に転送、コピーする指令を入力すると、CPU１２は、ステップＳ１１において、インタフェース１７を介してディスプレイ３にコピーする曲を選択するためのGUI（Graphical User Interface）を表示させる。

【００２１】

具体的には、例えば、CPU１２は、CD-ROMドライブ１４に装着されたCDのTOC（Table Of Contents）を読み込み、そのCDに含まれる曲の情報を得て、ディスプレイ３に表示させる。または、CPU１２は、CDに含まれている各曲毎のISRC（International Standard Recording Code）を読み出し、その曲の情報を得て、ディスプレイ３に表示させる。あるいはまた、CPU１２は、インターネット４を介して外部のデータベースにアクセスし、TOCを用いて、そのCDの曲の情報を得て、対応するGUIをディスプレイ３に表示させる。ユーザは、ディスプレイ３のGUIを利用して入力部２を操作し、コピーする曲を選択する。

【００２２】

次に、ステップＳ１２において、CPU１２は、ハードディスク１５に記憶されている期限データベースをチェックする。この期限データベースチェック処理の詳細は、図３のフローチャートに示されている。

【００２３】

ステップＳ３１においてCPU１２は、アダプタ７のCPU３２と共働して、期限データベース全体のハッシュ値を計算し、ステップＳ３２において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【００２４】

すなわち、ハードディスク１５には、期限データベースが形成されており、こ

の期限データベースには、図４に示すように、ハードディスク１５に記録されている音楽データを管理する管理情報として、過去に記録されたことのある曲のISRC番号とコピー日時が対応して記憶されている。この例においては、アイテム１乃至アイテム３の３つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全ての曲のISRC番号とコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップＳ３８において、アダプタ７のCPU３２により計算され、不揮発性メモリ３４に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA，MD５などがある。CPU１２は、ステップＳ３１において、CPU３２が実行したのと同様にハッシュ値を計算する。そして、ステップＳ３２において、CPU１２は、CPU３２に、不揮発性メモリ３４に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップＳ３１で、いま自分自身が計算したハッシュ値とを比較する。

【００２５】

ステップＳ３３において、CPU１２は、ステップＳ３１でいま計算したハッシュ値と、不揮発性メモリ３４に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、CPU１２は、ステップＳ３４において、例えば、「期限データベースが改竄されたので、コピーができません」といったメッセージを発生し、インタフェース１７を介してディスプレイ３に出力し、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されている音楽データを再生し、ハードディスク１５にコピーする処理が禁止される。

【００２６】

ステップＳ３１で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップＳ３５に進み、CPU１２は、ステップＳ１１で指定されたコピーする曲として選択された曲（選択曲）のISRC番号をCDから取得する。CDにISRC番号が記録されていない場合、CPU１２は、そのCDのTOCのデータを読み出し、その

データにハッシュ関数を適用するなどして、例えば、５８ビットなどの適当な長さのデータを得て、これをISRC番号に代えて用いる。

【００２７】

ステップＳ３６において、CPU１２は、ステップＳ３５で取得したISRC番号（すなわち、選択曲）が期限データベース（図４）に登録されているか否かを判定する。ISRC番号が期限データベースに登録されていない場合には、その曲はまだハードディスク１５に記録されていないことになるので、ステップＳ３７に進み、CPU１２は、その曲のISRC番号と現在の日時とを期限データベースに登録する。なお、CPU１２は、この現在の日時として、CPU３２から転送を受けた、アダプタ７のRTC３５が出力する値を利用する。そして、ステップＳ３８において、CPU１２は、その時点における期限データベースのデータを読み出し、アダプタ７のCPU３２に転送する。CPU３２は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ３４に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップＳ３２において、前回保存しておいたハッシュ値として利用される。

【００２８】

次に、ステップＳ３９において、CPU１２は、選択曲が期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図２のステップＳ１３において、選択曲が期限データベースに登録されているか否かの判定を行うときに用いられる。

【００２９】

ステップＳ３６において、選択曲のISRC番号が期限データベースに登録されていると判定された場合、その選択曲は、少なくとも一度、ハードディスク１５に登録されたことがある曲であるということになる。そこで、この場合、ステップＳ４０に進み、CPU１２は、期限データベースに登録されているその選択曲の登録日時より、現在の日時（アダプタ７のRTC３５が出力した現在の日時）が４８時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に４８時間以上経過している場合には、ハードディスク１５に、少なくとも一度は記録したことがあるが、既に、その時から４８時間以上経過しているので、その曲を

再度コピーさせたとしても、それほど実害がないので、この場合には、ハードディスク１５へのコピーが許容される。そこで、ステップＳ４１に進み、CPU１２は、期限データベースの日時を、過去の登録日時から現在の日時（RTC３５の出力する日時）に変更させる。そして、ステップＳ３８に戻り、CPU１２は、再び、期限データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させるとともに、ステップＳ３９において、その曲に対して未登録のフラグを設定する。

【００３０】

一方、ステップＳ４０において、現在時刻が登録日時より、まだ４８時間以上経過していないと判定された場合、その選択曲のハードディスク１５へのコピーが禁止される。そこで、この場合には、ステップＳ４２に進み、CPU１２は、その選択曲に対応して登録済みのフラグを設定する。

【００３１】

以上のようにして、期限データベースチェック処理により、選択曲がハードディスク１５に登録されているか否かを表すフラグが設定される。

【００３２】

図２に戻り、ステップＳ１３においてCPU１２は、選択曲が期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択曲が登録済みである場合には、ステップＳ１４に進み、CPU１２は、ディスプレイ３に、例えば、「この曲は一度コピーされてからまだ４８時間以上経過していないので、コピーすることができません」のようなメッセージを表示させる。これにより、ユーザは、その曲をハードディスク１５にコピーすることができない理由を知ることができる。

【００３３】

ステップＳ１３において、選択した曲が期限データベースに登録されていないと判定された場合、ステップＳ１５に進み、CPU１２は、CD-ROMドライブ１４を制御し、そこに装着されているCDから音楽データを読み出させる。この音楽データには、図５に示すように、所定の位置にウォータマークコードが挿入されている。CPU１２は、ステップＳ１６において、音楽データに含まれているウォータ

マークコードを抽出し、そのウォータマークコードがコピー禁止を表しているいるか否かをステップＳ１７において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップＳ１８に進み、CPU１２は、インタフェース１７を介してディスプレイ３に、例えば、「コピーは禁止されています」のようなメッセージを表示させ、コピー処理を終了させる。

【００３４】

これに対して、ステップＳ１７において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ１９に進み、CPU１２は、音楽データを、例えば、ATRAC（Adaptive Transform Acoustic Coding）（商標）などの方式で、ソフトウェア処理により圧縮させる。ステップＳ２０において、CPU１２は、予め設定され、メモリ１３に記憶されている暗号鍵を用いて、例えば、DES（Data Encryption Standard）方式、FEAL（Fast Encripherment Algotithm）方式などの暗号化方法により、音楽データを暗号化する。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ７のCPU３２により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ１だけではなく、それに付随して装着されたハードウェアとしてのアダプタ７のCPU３２と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【００３５】

次に、ステップＳ２１において、CPU１２は、暗号化されたデータをハードディスク１５に転送し、１つのファイルとしてファイル名を付けて保存させる。あるいはまた、１つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

【００３６】

この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【００３７】

さらに、ステップＳ２２において、CPU１２は、予め定められているメモリ１３に記憶されている保存用鍵を使って、上述したDES方式、FEAL方式などの方式

で、音楽データを暗号化した暗号鍵を暗号化し、ハードディスク１５の曲データベースに保存する。

【００３８】

ステップＳ２３において、CPU１２は、保存したファイルに関する情報、暗号化された暗号鍵、その曲の情報、ユーザがGUIを介して入力した曲名の情報の要素を組にしてハードディスク１５の曲データベースに登録する。そして、ステップＳ２４において、CPU１２は、CPU３２に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。

【００３９】

このようにして、例えば、図６に示すような曲データベースが、ハードディスク１５上に登録される。この例においては、アイテム１乃至アイテム３のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【００４０】

次に、図７乃至図９のフローチャートを参照して、ハードディスク１５からメモリスティックウォークマン６の不揮発性メモリ２３（メモリスティック）に、音楽データを移動する処理について説明する。ステップＳ５１において、CPU１２は、曲データベース全体のハッシュ値を計算し、ステップＳ５２で、前回CPU３２に計算させ、不揮発性メモリ３４に保存しておいたハッシュ値と比較する。両者が一致しない場合、CPU１２は、ステップＳ５３に進み、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ３に表示させた後、処理を終了させる。この場合の処理は、図３のステップＳ３１乃至ステップＳ３４の処理と同様の処理である。この場合においては、ハードディスク１５からメモリスティックウォークマン６への音楽データの移動が実行されないことになる。

【００４１】

次に、ステップＳ５４において、CPU１２は、ハードディスク１５に形成されている曲データベースから、そこに登録されている曲の情報を読み出し、ディス

プレイ３に、選択のためのGUIとして表示させる。ユーザは、この選択のためのGUIに基づいて、ハードディスク１５からメモリスティックウォークマン６へ移動させる曲を、入力部２を操作して選択する。次に、ステップＳ５５において、CPU１２は、ステップＳ５４で選択された選択曲の再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図１０のフローチャートを参照して後述する。

【００４２】

次に、ステップＳ５６において、パーソナルコンピュータ１のCPU１２とメモリスティックウォークマン６の認証装置２２との間において、相互認証処理が行われ、通信用鍵が共有される。

【００４３】

例えば、メモリスティックウォークマン６の不揮発性メモリ２３には、マスター鍵ＫＭが予め記憶されており、パーソナルコンピュータ１のメモリ１３には、個別鍵ＫＩとIDが予め記憶されているものとする。認証装置２２は、CPU１２から、メモリ１３に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫＭにハッシュ関数（ＳＨＡなどのハッシュ関数またはＤＥＳなどでも良い）を適用して、メモリ１３に記憶されているパーソナルコンピュータ１の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ１とメモリスティックウォークマン６の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【００４４】

あるいはまた、パーソナルコンピュータ１のメモリ１３にIDとマスター鍵ＫＭＰを予め記憶させておくとともに、メモリスティックウォークマン６の不揮発性メモリ２３にもメモリスティックウォークマン６のIDとマスター鍵ＫＭＭを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【００４５】

なお、認証の方法としては、例えば、IOS（International Organization for Standardization）　９７９８－２を利用することができる。

【００４６】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップＳ５７において、CPU１２は、選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データ（例えば、図２のステップＳ２０の処理で暗号化されている）をハードディスク１５から読み出す。ステップＳ５８において、CPU１２は、ステップＳ５７で読み出したデジタル音楽データの圧縮符号化方式（ステップＳ１９の処理）、暗号化方式（ステップＳ２０の処理）、フォーマットなどをメモリスティックウォークマン６のものに変換する処理を実行する。この変換処理の詳細は、図１２のフローチャートを参照して後述する。

【００４７】

ステップＳ５９において、CPU１２は、ステップＳ５８で変換した音楽データを、ステップＳ５６の相互認証処理により共有した通信用鍵で暗号化し、メモリスティックウォークマン６にインタフェース１７を介して転送する。ステップＳ６０において、メモリスティックウォークマン６の認証装置２２は、インタフェース２１を介してこの伝送されてきた音楽データを受信すると、その音楽データを、そのまま不揮発性メモリ２３に記憶させる。

【００４８】

ステップＳ６１において、CPU１２は、さらに、曲データベースに登録されているその選択曲の再生条件（開始日時、終了日時、回数制限など）を、メモリスティックウォークマン６が管理している形式に変換する。ステップＳ６２において、CPU１２は、さらに選択曲の曲データベース中に登録されているコピー条件中のSCMS情報を、メモリスティックウォークマン６の管理する形式に変換する。そして、ステップＳ６３において、CPU１２は、ステップＳ６１で変換した再生条件と、ステップＳ６２で変換したSCMS情報を、メモリスティックウォークマン６に転送する。メモリスティックウォークマン６の認証装置２２は、転送を受け

た再生条件とSCMS情報を、不揮発性メモリ２３に保存する。

【００４９】

ステップＳ６４において、CPU１２はまた、選択曲の曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU１２が曲データベース中で扱っている形式のまま、メモリスティックウォークマン６に転送し、不揮発性メモリ２３に保存させる。

【００５０】

ステップＳ６５において、CPU１２は、選択曲の暗号化されている暗号鍵を曲データベースから読み出し、ステップＳ６６において、その暗号鍵をメモリ１３に保存されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化した暗号鍵を、CPU１２は、メモリスティックウォークマン６に転送する。

【００５１】

メモリスティックウォークマン６の認証装置２２は、ステップＳ６７で、パーソナルコンピュータ１から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、不揮発性メモリ２３に保存する。

【００５２】

認証装置２２は、暗号鍵の保存が完了すると、ステップＳ６８において、パーソナルコンピュータ１に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ１のCPU１２は、メモリスティックウォークマン６からこの通知を受けると、ステップＳ６９において、ハードディスク１５から、その音楽データのファイルを削除するとともに、曲データベースからその曲の要素の組を削除する。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップＳ７０において、CPU１２は、アダプタ７のCPU３２に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。このハッシュ値が、上述したステップＳ５２において、前回保存しておいたハッシュ値として用いられることになる。

【００５３】

次に、図７のステップＳ５５における選択曲の再生条件などのチェック処理について説明する。ステップＳ８１において、CPU１２は、曲データベースから、各種の条件を読み出す。CPU１２は、ステップＳ８２において、ステップＳ８１で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップＳ８３に進み、CPU１２は、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ３に表示させ、処理を終了させる。ステップＳ８２において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップＳ８４に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ７のRTC３５より出力されたものが用いられる。これにより、ユーザが、パーソナルコンピュータ１の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。CPU１２は、この現在日時をCPU３２から提供を受けて、ステップＳ８４の判断を自ら行うか、または、ステップＳ８１で、曲データベースから読み出した再生条件をアダプタ７のCPU３２に供給し、CPU３２に、ステップＳ８４の判定処理を実行させる。

【００５４】

現在日時が再生終了日時を過ぎている場合、ステップＳ８５に進み、CPU１２は、選択曲をハードディスク１５から消去するとともに、曲データベースから、その選択曲の情報を消去する。ステップＳ８６において、CPU１２は、CPU３２に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ３４に保存させる。以後、処理は終了される。従って、この場合、音楽データの移動が実行されない。

【００５５】

ステップＳ８４において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップＳ８７に進み、CPU１２は、その選択曲の再生時課金条件（例えば、再生１回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、CPU１２は、ステップＳ８８において、メモリスティックウォークマン６と通信し、メモリスティックウ

ォークマン６に課金機能が存在するか否かを判定する。メモリスティックウォークマン６に課金機能が存在しない場合には、選択曲をメモリスティックウォークマン６に転送する訳にはいかないので、ステップＳ８９において、CPU１２は、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ３に表示させ、音楽データの移動処理を終了させる。

【００５６】

ステップＳ８７において再生時課金条件が登録されていないと判定された場合、または、ステップＳ８８において、メモリスティックウォークマン６に課金機能が存在すると判定された場合、ステップＳ９０に進み、CPU１２は、選択曲に関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップＳ９１に進み、CPU１２は、メモリスティックウォークマン６に、その再生条件を守る機能が存在するか否かを判定する。メモリスティックウォークマン６が、その再生条件を守る機能を有していない場合には、ステップＳ９２に進み、CPU１２は、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ３に表示させ、処理を終了させる。

【００５７】

ステップＳ９０において、再生条件が登録されていないと判定された場合、またはステップＳ９１において、メモリスティックウォークマン６が再生条件を守る機能を有している判定された場合、再生条件等のチェック処理が終了され、図７のステップＳ５６に戻る。

【００５８】

図１１は、メモリスティックウォークマン６が管理している（守ることが可能な）再生条件の例を表している。この例においては、アイテム１乃至アイテム３の各曲について、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム２についてのみ登録されており、アイテム１とアイテム３については登録されていない。従って、アイテム２の曲が選択曲とされた場合、再生回数の再生条件は守ることが可能であるが、アイテム１またはアイテム３の曲が選択曲とされた場合、再生回数の条件は守ることができないことになる。

【００５９】

次に、図１２のフローチャートを参照して、図７のステップＳ５８におけるフォーマット変換処理の詳細について説明する。ステップＳ１０１において、CPU１２は、ハードディスク１５に記録されている選択曲のフォーマット（再生条件、使用条件、コピー条件など）を調べる。ステップＳ１０２において、CPU１２は、相手先の機器（今の場合、メモリスティックウォークマン６）に設定することが可能な条件を調べる。すなわち、CPU１２は、メモリスティックウォークマン６の認証装置２２に設定可能な条件を問い合わせ、その回答を得る。ステップＳ１０３においてCPU１２は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップＳ１０２で調べた条件に基づいて決定する。

【００６０】

ステップＳ１０４において、CPU１２は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップＳ１０５に進み、音楽データをメモリスティックウォークマン６に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をメモリスティックウォークマン６が守ることができないので、そのようなメモリスティックウォークマン６には、音楽データを移動することが禁止されるのである。

【００６１】

ステップＳ１０４において設定可能な条件が存在すると判定された場合、ステップＳ１０６に進み、CPU１２は、その条件を相手先の機能フォーマットの条件に変換する。そして、ステップＳ１０７において、変換した条件を相手先の機器に設定する。その結果、メモリスティックウォークマン６は、設定された条件に従って（その条件を守って）、音楽データ再生することが可能となる。

【００６２】

次に、図１３乃至図１５のフローチャートを参照して、ハードディスク１５からメモリスティックウォークマン６に音楽データをコピーする場合の処理について説明する。この図１３乃至図１５のステップＳ１１１乃至ステップＳ１２７の処理は、図７乃至図９のハードディスク１５からメモリスティックウォークマン

６へ音楽データを移動させる場合のステップＳ５１乃至ステップＳ６７の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択曲の再生条件とのチェック処理が行われる。さらに、メモリスティックウォークマン６と、パーソナルコンピュータ１との間の相互認証処理の後、音楽データが、パーソナルコンピュータ１のハードディスク１５からメモリスティックウォークマン６の不揮発性メモリ２３に転送され、保存される。その後、ステップＳ１２８において、パーソナルコンピュータ１のCPU１２は、曲データベースのコピー回数カウンタを１だけインクリメントする。そして、ステップＳ１２９において、CPU１２は、CPU３２に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ３４に保存させる。

【００６３】

次に、図１６のフローチャートを参照して、メモリスティックウォークマン６からハードディスク１５に音楽データを移動する処理について説明する。ステップＳ１６１において、パーソナルコンピュータ１のCPU１２は、メモリスティックウォークマン６の認証装置２２に対して不揮発性メモリ２３に記憶されている曲の情報の読み出しを要求する。認証装置２２は、この要求に対応して、不揮発性メモリ２３に記憶されている曲の情報をパーソナルコンピュータ１に送信する。パーソナルコンピュータ１のCPU１２は、この情報に基づいて、ディスプレイ３に、不揮発性メモリ２３に記憶されている曲を選択するためのGUIを表示させる。ユーザは、入力部２を操作して、そのGUIに基づいて、メモリスティックウォークマン６からハードディスク１５に移動させる曲を指定する。

【００６４】

ステップＳ１６２において、CPU１２は、認証装置２２との間において、相互認証処理を実行し、通信用鍵を共有する。この処理は、図７のステップＳ５６における場合と同様の処理である。

【００６５】

次に、ステップＳ１６３において、認証装置２２は、不揮発性メモリ２３に記憶されている暗号化されている選択曲の音楽データを読み出し、パーソナルコンピュータ１に転送する。パーソナルコンピュータ１のCPU１２は、ステップＳ１

６４において、メモリスティックウォークマン６から転送されてきた音楽データを、１つのファイルとしてファイル名を付けて、ハードディスク１５に保存する。この保存は、例えば、１つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【００６６】

ステップＳ１６５において、認証装置２２は、不揮発性メモリ２３に記憶されている選択曲の暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ１に転送する。この暗号鍵は、例えば、図９のステップＳ６７の処理で不揮発性メモリ２３に保存されていたものである。

【００６７】

ステップＳ１６６において、パーソナルコンピュータ１のCPU１２は、メモリスティックウォークマン６から暗号鍵の転送を受けると、それを通信用鍵で復号し、自分自身の保存用鍵で暗号化する。ステップＳ１６７で、CPU１２は、ステップＳ１６４で保存した音楽データのファイルのファイル名、その曲の情報をユーザがGUIを介して入力した曲名、ステップＳ１６６で暗号化した暗号鍵などを、ハードディスク１５の曲データベースに登録する。そして、ステップＳ１６８において、CPU１２は、その曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させる。

【００６８】

ステップＳ１６９において、パーソナルコンピュータ１のCPU１２は、メモリスティックウォークマン６に対して暗号鍵が保存されたことを通知し、その曲の音楽データの削除を要求する。認証装置２２は、パーソナルコンピュータ１から、その曲の音楽データの削除が要求されてきたとき、ステップＳ１７０において、不揮発性メモリ２３に記憶されているその曲の音楽データを削除する。

【００６９】

次に、メモリスティックウォークマン６からハードディスク１５へ音楽データをコピーする場合の処理について、図１７のフローチャートを参照して説明する。この図１７に示すステップＳ１８１乃至ステップＳ１８８の処理は、図１６の

メモリスティックウォークマン６からハードディスク１５へ音楽データを移動させる場合の処理におけるステップＳ１６１乃至ステップＳ１６８の処理と同様の処理である。すなわち、コピー処理の場合は、図１６のステップＳ１６９，Ｓ１７０の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【００７０】

次に、図１８のフローチャートを参照して、EMDサーバ５から転送を受けた音楽データをハードディスク１５にコピーする処理について説明する。ステップＳ２０１において、CPU１２は、入力部２を介してユーザからEMDサーバ５へのアクセスが指令されたとき、インターネット接続インタフェース１１を制御し、インターネット４を介してEMDサーバ５にアクセスさせる。EMDサーバ５は、このアクセスに対応して、自分自身が保持している曲の曲番号、曲名、各情報などの情報を、インターネット４を介してパーソナルコンピュータ１に転送する。パーソナルコンピュータ１のCPU１２は、インターネット接続インタフェース１１を介して、この情報を取得したとき、それをインタフェース１７を介してディスプレイ３に表示させる。ユーザは、ディスプレイ３に表示されたGUIを利用して、ステップＳ２０２において、コピーを希望する曲を指定する。この指定情報は、インターネット４を介してEMDサーバ５に転送される。ステップＳ２０３において、CPU１２は、EMDサーバ５との間において、インターネット４を介して相互認証処理を実行し、通信用鍵を共有する。

【００７１】

パーソナルコンピュータ１とEMDサーバ５との間で行われる相互認証処理は、例えば、ISO　９７９８－３で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ１は、自分自身の秘密鍵とEMDサーバ５の公開鍵を予め有しており、EMDサーバ５は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ１の公開鍵は、EMDサーバ５から転送したり、あるいはパーソナルコンピュータ１に予め配布されているcertificateをパーソナルコンピュータ１からEMDサーバ５に転送し、そのcretificateをEMDサーバ５が確認し、公開鍵を得るようにしてもよい。さらに、ステッ

プＳ２０４において、CPU１２は、EMDサーバ５との間において課金に関する処理を実行する。この課金の処理の詳細は、図１９のフローチャートを参照して後述する。

【００７２】

次に、ステップＳ２０５において、EMDサーバ５は、パーソナルコンピュータ１に対して、ステップＳ２０２で指定された曲の暗号化されている音楽データをインターネット４を介してパーソナルコンピュータ１に転送する。このとき、時刻情報も適宜転送される。ステップＳ２０６において、CPU１２は、転送を受けた音楽データをファイル名を付けてハードディスク１５に１つのファイルとして保存する。ステップＳ２０７において、EMDサーバ５は、さらに、その曲の暗号鍵をステップＳ２０３でパーソナルコンピュータ１と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ１へ転送する。

【００７３】

CPU１２は、ステップＳ２０８において、EMDサーバ５より転送を受けた暗号鍵を単独で、またはアダプタ７のCPU３２と共同して通信用鍵を用いて復号し、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化する。ステップＳ２０９において、CPU１２は、その曲のファイル名、曲の情報、ユーザが入力した曲名、暗号化された暗号鍵を組にして、ハードディスク１５の曲データベースに登録する。さらに、ステップＳ２１０において、CPU１２は、その曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させる。

【００７４】

なお、ステップＳ２０５においてEMDサーバ５は、音楽データとともに、時刻データをパーソナルコンピュータ１に送信する。この時刻データは、パーソナルコンピュータ１からアダプタ７に転送される。アダプタ７のCPU３２は、パーソナルコンピュータ１より転送されてきた時刻データを受信すると、ステップＳ２１１において、RTC３５の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ７のRTC３５の時刻情報を修正するようにしたので、アダプタ７を常に正しい時刻情報を保持することが可能となる。

【００７５】

また、RTC３５を利用する処理を、後述する暗号化されたソースプログラムまたはオブジェクトプログラムでのみ実行させるようにすれば、時刻情報の改竄が困難になる。

【００７６】

次に、図１９のフローチャートを参照して、図１８のステップＳ２０４における課金に関する処理の詳細について説明する。ステップＳ２２１において、パーソナルコンピュータ１のCPU１２は、ステップＳ２０１でEMDサーバ５から伝送されてきた価格情報の中から、ステップＳ２０２で指定された選択曲の価格情報を読み取り、これをハードディスク１５上の課金ログに書き込む。図２０は、このような課金ログの例を表している。この例においては、ユーザは、アイテム１乃至アイテム３を、EMDサーバ５からコピーしており、アイテム１とアイテム２の領域は５０円とされ、アイテム３の料金は６０円とされている。その時点における課金ログのハッシュ値も、CPU３２により計算され、不揮発性メモリ３４に登録されている。

【００７７】

次に、ステップＳ２２２において、パーソナルコンピュータ１のCPU１２は、ステップＳ２２１で書き込んだ課金ログをハードディスク１５から読み出し、これをインターネット４を介してEMDサーバ５に転送する。EMDサーバ５は、ステップＳ２２３において、パーソナルコンピュータ１から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ５は、内蔵するデータベースに、パーソナルコンピュータ１のユーザから伝送されてきた課金ログを追加更新する。そして、ステップＳ２２４において、EMDサーバ５は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップＳ２２５に進み、EMDサーバ５は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップＳ２２６において、決裁サーバは、パーソナルコンピュータ１のユーザに対する決裁処理を実行する。ステップＳ２２４において、決裁は直ちには行われないと判定された場合、ステップＳ２２５とＳ２２６の処理はスキップされる。すなわち、この処理は、例えば、月に１回など

、定期的にその後実行される。

【００７８】

次に、図２１と図２２のフローチャートを参照して、音声入出力インタフェース１６のIEC６０９５８端子１６ａから入力された、図示せぬCDプレーヤなどからの再生音楽データを、ハードディスク１５にコピーする場合の処理について説明する。ステップＳ２４１において、ユーザは、CDプレーヤのIEC６０９５８出力端子を、パーソナルコンピュータ１の音声入出力インタフェース１６のIEC６０９５８端子１６ａに接続する。ステップＳ２４２において、ユーザは、入力部２を操作し、CDプレーヤからコピーする曲の曲名を入力する。そして、ステップＳ２４３においてユーザは、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ１との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ１の入力部２を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【００７９】

CDプレーヤにおいて、CDの再生が開始されると、ステップＳ２４４において、CDプレーヤから出力された音楽データが、IEC６０９５８端子１６ａを介してパーソナルコンピュータ１に転送されてくる。ステップＳ２４５において、CPU１２は、IEC６０９５８端子１６ａを介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー１回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップＳ２４６において、CPU１２は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップＳ２４７に進み、CPU１２は、ディスプレイ３に、例えば、「コピーが禁止されています」といったメッセージを表示させ、コピー処理を終了する。すなわち、この場合には、ハードディスク１５へのコピーが禁止される。

【００８０】

CPU１２は、ステップＳ２４６において、ステップＳ２４５で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップＳ２４８に進み、ウ

ォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップＳ２４９において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップＳ２４７に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【００８１】

ステップＳ２４９において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ２５０に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択曲が既に登録されていれば、ステップＳ２５１，Ｓ２５２の処理で、処理が終了される。この処理は、図２のステップＳ１３，Ｓ１４の処理と同様の処理である。

【００８２】

選択曲がまだハードディスク１５に登録されていない曲であれば、ステップＳ２５３乃至Ｓ２５８で、その登録処理が実行される。このステップＳ２５３乃至ステップＳ２５８の処理は、ステップＳ２５７において、IEC６０９５８端子から供給されてくるSCMS情報も曲データベースに登録される点を除き、図２のステップＳ１９乃至ステップＳ２４の処理と同様の処理であるので、その説明は省略する。

【００８３】

次に、図２３と図２４のフローチャートを参照して、音楽データをハードディスク１５からIEC６０９５８端子１６ａに出力（再生）する場合の処理について説明する。ステップＳ２７１乃至ステップＳ２７３において、図１３のステップＳ１１１乃至Ｓ１１３における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップＳ２７４に進み、CPU１２は、ハードディスク１５の曲データベースにアクセスし、そこに登録されている曲の情報を読み出し、ディスプレイ３に表示させる。ユーザは、その表示を見て、入力部２を適宜操作して、再生出力する曲を選択する。ステップＳ２７５において、CPU１２は、選択曲の再生条件等のチェック処理を実行する。この再生条件等のチェック処

理の詳細は、図２５のフローチャートを参照して後述する。

【００８４】

次に、ステップＳ２７６において、CPU１２は、ステップＳ２７４において選択された曲の暗号鍵を曲データベースから読み出し、保存用鍵で復号する。ステップＳ２７７において、CPU１２は、選択曲のSCMS情報を曲データベースから読み出し、IEC６０９５８端子から出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は１だけインクリメントされ、新たなSCMS情報とされる。ステップＳ２７８において、CPU１２はさらに、選択曲のISRCを曲データベースから読み出す。

【００８５】

次に、ステップＳ２７９において、CPU１２は、曲データベースから選択曲ファイル名を読み出し、そのファイル名を基に、その音楽データをハードディスク１５から読み出す。CPU１２はさらに、その音楽データに対応する暗号鍵を曲データベースから読み出し、保存用鍵で復号し、復号した暗号鍵を用いて、暗号化されている音楽データを復号する。CPU１２は、さらに、その音楽データの圧縮符号を復号する。ステップＳ２８０において、CPU１２は、ステップＳ２７９で、復号したデジタル音楽データを、ステップＳ２７７で決定したSCMS情報、並びにステップＳ２７８で読み出したISRC情報とともに、IEC６０９５８の規定に従って、IEC９０９５８端子１６ａから出力する。さらにまた、デジタル音楽データをアナログ化し、音声入出力インタフェース１６のアナログ出力端子から出力する。

【００８６】

ステップＳ２８１において、CPU１２は、曲データベース中の再生回数カウンタの値を１だけインクリメントする。そして、ステップＳ２８２において、選択曲に再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ２８３に進み、CPU１２は、対応する料金を課金ログに書き込み、ステップＳ２８４において、曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に記憶させる。ステップＳ２８２において、選択曲に再生時課金条件が付加されていないと判定された場合、ステ

ップＳ２８３とステップＳ２８４の処理はスキップされる。

【００８７】

次に、図２５のフローチャートを参照して、図２３のステップＳ２７５の再生条件等のチェック処理の詳細について説明する。ステップＳ３０１において、CPU１２は、曲データベースの各種条件を読み出す。ステップＳ３０２においてCPU１２は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップＳ３０３に進み、選択曲をハードディスク１５から削除させるとともに、曲データベースから選択曲の情報を削除させる。ステップＳ３０４において、CPU１２はさらに、曲データベースの新たなハッシュ値をCPU３２に計算させ、そのハッシュ値を不揮発性メモリ３４に保存させる。この場合、再生出力は禁止される。

【００８８】

ステップＳ３０２において、再生回数が制限回数を過ぎていないと判定された場合、ステップＳ３０５に進み、CPU１２は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップＳ３０３において、選択曲をハードディスクから削除させるとともに、曲データベースからも削除させる。そして、ステップＳ３０４において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【００８９】

ステップＳ３０５において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップＳ３０６に進み、CPU３２は、その選択曲に対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ３０７に進み、CPU１２は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ３に表示させる。ステップＳ３０６において、再生時課金条件が付加されていないと判定された場合、ステップＳ３０７の処理はスキップされる。

【００９０】

次に、図２６と図２７のフローチャートを参照して、ハードディスク１５から

メモリスティックウォークマン６経由で音楽データを出力（再生）する場合の処理について説明する。ステップＳ３２１乃至ステップＳ３２５において、曲データベースの改竄チェックと選択曲の指定、並びに選択曲の再生条件等のチェック処理が行われる。その処理は、図２３のステップＳ２７１乃至ステップＳ２７５の処理と同様の処理であるので、その説明は省略する。

【００９１】

ステップＳ３２６において、メモリスティックウォークマン６とパーソナルコンピュータ１の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップＳ３２７において、パーソナルコンピュータ１のCPU１２は、メモリスティックウォークマン６に対して、これから送る暗号化音声データを再生するように命令する。ステップＳ３２８において、CPU１２は、ステップＳ３２４で指定された選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データをハードディスク１５から読み出す。CPU１２は、ステップＳ３２９において、音楽データの圧縮符号化方式、暗号化方式、フォーマットなどをメモリスティックウォークマン６の方式のものに変換する処理を実行する。そして、ステップＳ３３０において、CPU１２は、ステップＳ３２９において変換した音楽データを通信用鍵で暗号化し、メモリスティックウォークマン６に転送する。

【００９２】

ステップＳ３３１において、メモリスティックウォークマン６の認証装置２２は、ステップＳ３２７において、パーソナルコンピュータ１から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップＳ３３２において、CPU１２は、曲データベースの再生回数カウントを１だけインクリメントする。さらに、ステップＳ３３３において、CPU１２は、選択曲に再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップＳ３３４において、その料金を課金ログに書き込み、ステップＳ３３５において、CPU３２に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択曲に再生時課金条件が付加されていない場合には、ステップＳ３３４，ステップＳ３３５の処理はスキップされる。

【００９３】

本発明においては、音楽データが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU１２を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【００９４】

さらに、上述したように、CPU１２の機能の一部は、ハードウェアとしてのアダプタ７に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

【００９５】

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ７の不揮発性メモリ３４に保存される。すなわち、図３のステップＳ３２，Ｓ３３などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ３４に記憶されているものとされる。これにより、例えば、ハードディスク１５に保存されている音楽データを、他の記録媒体にコピーまたは移動させる前に、ハードディスク１５の記録内容をバックアップしておき、ハードディスク１５から、そこに保存されている音楽データを他の記録媒体にコピーまたはムーブした後、ハードディスク１５にバックアップしておいたデータを再びリストアするようにすることで、実質的に再現なく、コピーまたはムーブができてしまうようなことが防止される。

【００９６】

例えば、図２８に示すように、ハードディスク１５に曲Ａ，Ｂが保存されている場合、不揮発性メモリ３４には、曲Ａと曲Ｂの情報に対応するハッシュ値が保存されている。この状態において、ハードディスク１５の記録データを他の記録媒体５１にバックアップしたとする。その後、ハードディスク１５に保存されている曲Ａと曲Ｂのうち、曲Ａを他の記録媒体５２に移動させた場合、その時点において、ハードディスク１５に記録されている曲は、曲Ｂだけとなるので、不揮発性メモリ３４のハッシュ値も、曲Ｂに対応するハッシュ値に変更される。

【００９７】

従って、その後、記録媒体５１にバックアップしておいたハードディスク１５の内容をハードディスク１５にリストアして、ハードディスク１５に、再び曲Ａと曲Ｂを保存させたとしても、不揮発性メモリ３４には、曲Ｂの情報から演算されたハッシュ値が記憶されており、曲Ａと曲Ｂの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、ハードディスク１５に記憶されている曲Ａと曲Ｂに基づくハッシュ値が、不揮発性メモリ３４に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、ハードディスク１５に保存されている曲Ａと曲Ｂの利用が制限されてしまうことになる。

【００９８】

さらに、上述したように、アダプタ７は、RTC３５を内蔵しており、このRTC３５の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ５）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ１が管理するものではなく、RTC３５が出力するものが利用される。従って、ユーザが、パーソナルコンピュータ１の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【００９９】

また、アダプタ７は、暗号化されて転送されてきたプログラムをROM３６に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図２９のフローチャートを参照して説明する。

【０１００】

すなわち、パーソナルコンピュータ１は、アダプタ７に対して、所定の処理を実行させたいとき、ステップＳ３５１において、アダプタ７に実行させるべきプログラムをメモリ１３に予め記憶されている暗号鍵を用いて暗号化してアダプタ７に転送する。アダプタ７のROM３６には、パーソナルコンピュータ１から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラム

が予め記憶されている。CPU３２は、このROM３６に記憶されているプログラムに従って、パーソナルコンピュータ１から転送されてきた暗号化されているプログラムをステップＳ３５２において復号する。そして、ステップＳ３１３において、CPU３２は、復号したプログラムをRAM３３に展開し、ステップＳ３５４において、そのプログラムを実行する。

【０１０１】

例えば、上述したように、パーソナルコンピュータ１のCPU１２は、ハードディスク１５の曲データベースのハッシュ値をアダプタ７に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ７のCPU３２に転送する。CPU３２は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ３４に記憶させる。あるいは、そのハッシュ値を、CPU３２は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ１のCPU１２に転送する。

【０１０２】

図３０は、アダプタ７の内部のより具体的な構成を表している。アダプタ７は、半導体ICとして形成される。アダプタ７は、図１に示したインタフェース３１、CPU３２、RAM３３、不揮発性メモリ３４、RTC３５、ROM３６以外に、RAM３３に対する書き込みと読み出しを制御するRAMコントローラ６１、並びに論理回路６２を有している。論理回路６２は、例えば、暗号化されている音楽データを解読した後、解読したデータをアダプタ７から直接出力するような場合の処理のために用いられる。

【０１０３】

これらのインタフェース３１乃至ROM３６、RAMコントローラ６１、並びに論理回路６２は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【０１０４】

水晶振動子７１は、アダプタ７が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路７２は、RTC３５を動作させる

ための発振回路である。バッテリ７３は、発振回路７２、不揮発性メモリ３４、およびRTC３５に対してバックアップ用の電力を供給している。アダプタ７のその他の回路には、パーソナルコンピュータ１の電源供給回路８１からの電力が供給されている。

【０１０５】

不揮発性メモリ３４は、書き込み消去可能なROMで構成することも可能であるが、バッテリ７３からのバックアップ電源でバックアップされるRAMで構成する場合には、例えば、図３１に示すように、不揮発性メモリ３４の上に保護アルミニウム層９１を形成し、さらに、その保護アルミニウム層９１と同一平面上となるように、不揮発性メモリ３４にバッテリ７３からの電力を供給する電源パターン９２を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ３４を改竄すべく、保護アルミニウム層９１を削除しようとすると、同一平面上の電源パターン９２も削除されてしまい、不揮発性メモリ３４に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【０１０６】

さらに、図３２に示すように、不揮発性メモリ３４に対するデータの書き込みまたは読み出しのための配線１０１－１乃至１０１－３は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線１０１－３からデータを読み出すためには、上方の配線１０１－１，１０１－２を除去しなければならず、複数の配線１０１－１，１０１－２，１０１－３から同時にデータを読み取ることができなくなる。さらにまた、この配線１０１－１乃至１０１－３を冗長に形成し、直接プローブすると、その付加容量により、その内容を解析することが困難になるようにすることができる。

【０１０７】

次に、メモリスティックウォークマン６がパーソナルコンピュータ１から所定のデータを受け取る場合の、相互認証の処理を図３３および図３４のフローチャートを参照して説明する。ステップＳ４０１において、パーソナルコンピュータ

１のＣＰＵ１２は、乱数Ｎａを生成する。ステップＳ４０２において、パーソナルコンピュータ１のＣＰＵ１２は、インターフェース１７に、パーソナルコンピュータ１のID、鍵のカテゴリ番号Ｇ、および乱数Ｎａをメモリスティックウォークマン６へ送信させる。

【０１０８】

ステップＳ４２１において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎｂを生成する。ステップＳ４２２において、メモリスティックウォークマン６は、インターフェース３１を介して、パーソナルコンピュータ１から送信されたパーソナルコンピュータ１のID、鍵のカテゴリ番号Ｇ、および乱数Ｎａを受信する。ステップＳ４２３において、メモリスティックウォークマン６の認証装置２２は、鍵のカテゴリ番号Ｇから、マスター鍵ＫＭａの鍵番号ｊを求める。

【０１０９】

ステップＳ４２４において、メモリスティックウォークマン６の認証装置２２は、ｊ番目のマスター鍵ＫＭａ［ｊ］を求める。ステップＳ４２５において、メモリスティックウォークマン６の認証装置２２は、パーソナルコンピュータ１のIDに、マスター鍵ＫＭａ［ｊ］を基にしたＳＨＡなどのハッシュ関数を適用し、鍵Ｋａｂを求める。

【０１１０】

ステップＳ４２６において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎａ、乱数Ｎｂ、およびパーソナルコンピュータ１のIDに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４２７において、メモリスティックウォークマン６の認証装置２２は、乱数Ｓｂを生成する。

【０１１１】

ステップＳ４２８において、メモリスティックウォークマン６の認証装置２２は、インターフェース３１に、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ、および乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

【０１１２】

ステップＳ４０３において、パーソナルコンピュータ１は、インターフェース１７を介して、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ、および乱数Ｓｂを受信する。ステップＳ４０４において、パーソナルコンピュータ１のＣＰＵ１２は、鍵番号ｊを基に、個別鍵ＫＩａに含まれる鍵Ｋａｂを求める。ステップＳ４０５において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎａ、乱数Ｎｂ、およびパーソナルコンピュータ１のIDに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ２を求める。

【０１１３】

ステップＳ４０６において、パーソナルコンピュータ１のＣＰＵ１２は、受信した乱数Ｒ１と、ステップＳ４０５で生成した乱数Ｒ２とが等しいか否かを判定し、乱数Ｒ１と乱数Ｒ２とが等しくないと判定された場合、正当なメモリスティックウォークマンではないので、メモリスティックウォークマン６を認証せず、処理は終了する。ステップＳ４０６において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、メモリスティックウォークマン６は正当なメモリスティックウォークマンなので、ステップＳ４０７に進み、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｓａを生成する。

【０１１４】

ステップＳ４０８において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎｂおよび乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４０９において、パーソナルコンピュータ１のＣＰＵ１２は、インターフェース１７に、乱数Ｒ３および乱数Ｓｂをメモリスティックウォークマン６へ送信させる。ステップＳ４１０において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｓａおよび乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵Ｋｓを求める。

【０１１５】

ステップＳ４２９において、メモリスティックウォークマン６の認証装置２２は、インターフェース３１を介して、乱数Ｒ３および乱数Ｓｂを受信する。ステップＳ４３０において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎｂおよび乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用

し、乱数Ｒ４を求める。ステップＳ４３１において、メモリスティックウォークマン６の認証装置２２は、受信した乱数Ｒ３と、ステップＳ４３０で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４３１において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は正当なパーソナルコンピュータなので、ステップＳ４３２に進み、メモリスティックウォークマン６の認証装置２２は、乱数Ｓａおよび乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵Ｋｓを求める。

【０１１６】

以上のように、パーソナルコンピュータ１およびメモリスティックウォークマン６は、相互認証し、共通の一時鍵Ｋｓを得る。なお、ステップＳ４２５、ステップＳ４２６、ステップＳ４０５、ステップＳ４０８、ステップＳ４１０、ステップＳ４３０、およびステップＳ４３２において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

【０１１７】

次に、パーソナルコンピュータ１がメモリスティックウォークマン６に所定のデータを送信する場合の、相互認証の処理を図３４および図３６のフローチャートを参照して説明する。ステップＳ４５１において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎａを生成する。ステップＳ４５２において、パーソナルコンピュータ１は、インターフェース１７を介して、パーソナルコンピュータ１のID、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐ、メモリスティックウォークマン６の鍵のカテゴリ番号Ｇｓ、および乱数Ｎａをメモリスティックウォークマン６に送信する。

【０１１８】

ステップＳ４８１において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎｂを生成する。ステップＳ４８２において、メモリスティックウォークマン６は、インターフェース３１を介して、パーソナルコンピュータ１から送信されたパーソナルコンピュータ１のID、パーソナルコンピュータ１の鍵のカテ

ゴリ番号Ｇｐ、メモリスティックウォークマン６の鍵のカテゴリ番号Ｇｓ、および乱数Ｎａを受信する。ステップＳ４８３において、メモリスティックウォークマン６の認証装置２２は、メモリスティックウォークマン６の鍵のカテゴリ番号Ｇｓから、マスター鍵ＫＭａの鍵番号ｊを求める。

【０１１９】

ステップＳ４８４において、メモリスティックウォークマン６の認証装置２２は、ｊ番目のマスター鍵ＫＭａ［ｊ］を求める。ステップＳ４８５において、メモリスティックウォークマン６の認証装置２２は、パーソナルコンピュータ１のIDに、マスター鍵ＫＭａ［ｊ］を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋａｂを求める。ステップＳ４８６において、メモリスティックウォークマン６の認証装置２２は、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐを基に、マスター鍵ＫＩａの鍵番号ｋを求める。ステップＳ４８７において、メモリスティックウォークマン６の認証装置２２は、鍵Ｋａｂに、マスター鍵ＫＩａ［ｋ］を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋ’ａｂを求める。

【０１２０】

ステップＳ４８８において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎａおよび乱数Ｎｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４８９において、メモリスティックウォークマン６の認証装置２２は、乱数Ｓｂを生成する。

【０１２１】

ステップＳ４９０において、メモリスティックウォークマン６の認証装置２２は、インターフェース３１に、メモリスティックウォークマン６のID、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ、および乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

【０１２２】

ステップＳ４５３において、パーソナルコンピュータ１は、インターフェース１７を介して、メモリスティックウォークマン６のID、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ、および乱数Ｓｂを受信する。ステップＳ４５４において、パーソナルコ

ンピュータ１のＣＰＵ１２は、メモリスティックウォークマン６のIDに、パーソナルコンピュータ１のマスター鍵ＫＭＰを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵Ｋｍを求める。ステップＳ４５５において、パーソナルコンピュータ１のＣＰＵ１２は、ｊ番目の個別鍵ＫＩａを求める。ステップＳ４５６において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎａおよび乱数Ｎｂに、鍵ＫＩａを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋ’ａｂを求める。ステップＳ４５７において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎａおよび乱数Ｎｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ２を求める。

【０１２３】

ステップＳ４５８において、パーソナルコンピュータ１のＣＰＵ１２は、受信した乱数Ｒ１と、ステップＳ４５７で生成した乱数Ｒ２とが等しいか否かを判定し、乱数Ｒ１と乱数Ｒ２とが等しくないと判定された場合、正当なメモリスティックウォークマンではないので、メモリスティックウォークマン６を認証せず、処理は終了する。ステップＳ４５８において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、メモリスティックウォークマン６は正当なメモリスティックウォークマンなので、ステップＳ４５９に進み、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｓａを生成する。

【０１２４】

ステップＳ４６０において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｎｂおよび乱数Ｎａに、鍵ＫＩａを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４６１において、パーソナルコンピュータ１のＣＰＵ１２は、インターフェース１７を介して、メモリスティックウォークマン６に、乱数Ｒ３および乱数Ｓｂを送信する。ステップＳ４６２において、パーソナルコンピュータ１のＣＰＵ１２は、乱数Ｓａおよび乱数Ｓｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵Ｋｓを求める。

【０１２５】

ステップＳ４９１において、メモリスティックウォークマン６の認証装置２２は、インターフェース３１を介して、乱数Ｒ３および乱数Ｓｂを受信する。ステップＳ４９２において、メモリスティックウォークマン６の認証装置２２は、乱数Ｎｂおよび乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ４を求める。ステップＳ４９３において、メモリスティックウォークマン６の認証装置２２は、受信した乱数Ｒ３と、ステップＳ４９２で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４９３において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は、正当なパーソナルコンピュータなので、ステップＳ４９４に進み、メモリスティックウォークマン６の認証装置２２は、乱数Ｓａおよび乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵Ｋｓを求める。

【０１２６】

このように、パーソナルコンピュータ１およびメモリスティックウォークマン６は、相互認証し、共通の一時鍵Ｋｓを得る。図３５および図３６のフローチャートに示した手続きは、図３３および図３４のフローチャートに示す手続きよりも、いわゆる”なりすまし”に対する防御（検出）が強力である。なお、ステップＳ４８５、ステップＳ４８７、ステップＳ４８８、ステップＳ４５４、ステップＳ４５６、ステップＳ４５７、ステップＳ４６０、ステップＳ４６２、ステップＳ４９２、およびステップＳ４９４において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

【０１２７】

以上のように、パーソナルコンピュータ１およびメモリスティックウォークマン６は、相互認証の後に行われる処理に対応し、検出力が異なる相互認証の手続きを使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

【０１２８】

次に、ソースプログラムを暗号化する処理を、図３７のフローチャートを参照して説明する。ステップＳ５０１において、パーソナルコンピュータ１は、インターネット接続インターフェース１１を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップＳ５０２において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

【０１２９】

ステップＳ５０２において、受信したソースプログラムに改竄が発見さなかった場合、ステップＳ５０３に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップＳ５０４において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ１に送信する。ステップＳ５０５において、パーソナルコンピュータ１は、受信したソースプログラムを、ハードディスク１５に記録し、処理は終了する。

【０１３０】

以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、ＥＤＭサーバ５または所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

【０１３１】

次に、暗号化されたソースプログラムをアダプタ７が実行する処理を、図３８のフローチャートを参照して説明する。ステップＳ５２１において、アダプタ７のＣＰＵ３２は、パーソナルコンピュータ１から受信した、暗号化されたソースプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５２２において、アダプタ７のＣＰＵ３２は、インタープリタを起動し、復号されたソースプログラムを実行する。

【０１３２】

ステップＳ５２３において、アダプタ７のＣＰＵ３２は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ１に送信するか否かを判定し、結果をパーソナルコンピュータ１に送信しないと判定された場合、処理は終了

する。ステップＳ５２３において、結果をパーソナルコンピュータ１に送信すると判定された場合、ステップＳ５２４に進み、アダプタ７のＣＰＵ３２は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップＳ５２５において、アダプタ７のＣＰＵ３２は、インターフェース３１を介して、暗号化された結果をパーソナルコンピュータ１に送信し、処理は終了する。

【０１３３】

以上のように、アダプタ７は、暗号化されたソースプログラムを実行し、所定の場合、得られた結果を暗号化し、パーソナルコンピュータ１に送信する。

【０１３４】

なお、オブジェクトプログラムを暗号化し、暗号化されたオブジェクトプログラムをアダプタ７が実行するようにしてもよい。図３９は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップＳ５４１において、パーソナルコンピュータ１は、ソースプログラムをコンパイルし、所定のオブジェクトプログラムを生成する。ステップＳ５４２乃至ステップＳ５４６の処理は、図３７のステップＳ５０１乃至ステップＳ５０５とそれぞれ同様の処理なので、その説明は省略する。

【０１３５】

図４０は、暗号化されたオブジェクトプログラムをアダプタ７が実行する処理を説明するフローチャートである。ステップＳ５６１において、アダプタ７のＣＰＵ３２は、パーソナルコンピュータ１から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５６２において、アダプタ７のＣＰＵ３２は、復号されたオブジェクトプログラムをＲＡＭ３３に展開し、実行する。ステップＳ５６３乃至ステップＳ５６５は、図３８のステップ５２３乃至ステップＳ５２５とそれぞれ同様の処理なので、その説明は省略する。

【０１３６】

次に、オブジェクトプログラムを暗号化する他の処理を、図４１のフローチャートを参照して説明する。ステップＳ５８１において、パーソナルコンピュータ１のＣＰＵ１２は、ソースプログラムをコンパイルし、オブジェクトプログラム

を生成する。ステップＳ５８２において、パーソナルコンピュータ１のＣＰＵ１２は、インターフェース１７を介して、アダプタ７にアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖの発行を要求する。

【０１３７】

ステップＳ５８３において、パーソナルコンピュータ１は、インターフェース１７を介して、アダプタ７からアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖ（アダプタ７の不揮発性メモリ３４に記憶されている、アダプタ７固有の鍵Ｋｓを基に、生成される）を受信する。ステップＳ５８４において、パーソナルコンピュータ１のＣＰＵ１２は、オブジェクトプログラムをアプリケーション鍵Ｋａｐで暗号化する。ステップＳ５８５において、パーソナルコンピュータ１のＣＰＵ１２は、コンテキストに含まれるマスター鍵ＫＭｂなどを個別鍵Ｋｉｄｖで暗号化する。ステップＳ５８６において、パーソナルコンピュータ１のＣＰＵ１２は、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム、および個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵ＫＭｂなどをハードディスク１５に記録させ、処理は終了する。

【０１３８】

このように、パーソナルコンピュータ１は、アダプタ７から供給されたアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖで、オブジェクトプログラムおよびコンテキストを暗号化することができる。

【０１３９】

図４１のフローチャートに示される手順で暗号化されたオブジェクトプログラムをアダプタ７が実行する処理を、図４２のフローチャートを参照して説明する。ステップＳ６０１において、パーソナルコンピュータ１のＣＰＵ１２は、インターフェース１７を介して、アダプタ７に、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム、および個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵ＫＭｂなどを送信する。

【０１４０】

ステップＳ６０２において、アダプタ７のＣＰＵ３２は、不揮発性メモリ３４に予め記憶されている鍵Ｋｓおよびアプリケーション鍵Ｋａｐに、ハッシュ関数

を適用し、個別鍵Ｋｉｄｖを生成する。ステップＳ６０３において、アダプタ７のＣＰＵ３２は、受信したオブジェクトプログラムをアプリケーション鍵Ｋａｐで復号する。ステップＳ６０４において、アダプタ７のＣＰＵ３２は、コンテキストに含まれるマスター鍵ＫＭｂなどを個別鍵Ｋｉｄｖで復号する。

【０１４１】

ステップＳ６０５において、アダプタ７のＣＰＵ３２は、復号されたマスター鍵ＫＭｂなどを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップＳ６０６乃至ステップＳ６０８の処理は、図３８のステップＳ５２３乃至ステップＳ５２５とそれぞれ同様なので、その説明は省略する。

【０１４２】

以上のように、図４２のフローチャートで示される処理において、図４１のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ７は、暗号化されたオブジェクトプログラムを実行することができる。従って、図４１のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ７以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

【０１４３】

次に、アダプタ７がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ１のＣＰＵ１２に実行させるときの処理を図４３のフローチャートを参照して説明する。ステップＳ６５１において、アダプタ７のＣＰＵ３２は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

【０１４４】

この変換は、例えば、ＤＥＳの暗号化または復号のプログラムの場合、Feistel構造などの基本構造を繰り返す処理のとき、いわゆるＦ関数で利用される４８ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、ＤＥＳ　ＣＢＣ(Cipher Block Chaining)　Ｍｏｄｅで、多量のデータを復号するプログラムの場合、繰り返し構造の処理を順（シーケンシャル）に実行せず、多量のデータに対し、

複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

【０１４５】

また、例えば、ソースプログラムのインストラクションに対応するコード（例えば、加算を表すコードが”１”に対応し、乗算を表すコードが”２”に対応する）を毎回変更する。

【０１４６】

ステップＳ６５２において、アダプタ７のＣＰＵ３２は、変換された命令列を、インターフェース３１を介して、パーソナルコンピュータ１に送信する。

【０１４７】

ステップＳ６５３において、パーソナルコンピュータ１のＣＰＵ１２は、デシャッフルされた命令列を実行する。ステップＳ６５４において、パーソナルコンピュータ１のＣＰＵ１２は、命令列を実行して得られた処理結果をアダプタ７に送信する。

【０１４８】

ステップＳ６５５において、アダプタ７のＣＰＵ３２は、パーソナルコンピュータ１から受信した処理結果、およびアダプタ７のＣＰＵ３２が算出し保持している計算結果を基に、処理を継続する。ステップＳ６５６において、アダプタ７のＣＰＵ３２は、パーソナルコンピュータ１に処理を実行させるか否かを判定し、パーソナルコンピュータ１に処理を実行させないと判定された場合、処理は終了する。ステップＳ６５６において、パーソナルコンピュータ１に処理を実行させると判定された場合、手続きは、ステップＳ６５１に戻り、パーソナルコンピュータ１に処理を実行させる処理を繰り返す。

【０１４９】

以上のように、アダプタ７は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ１に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することができる。

【０１５０】

アダプタ７は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ１に送信することにより、オブジェクトプログラムの解読が困難

になる。アダプタ７が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ１に送信すれば、オブジェクトプログラムの解読は更に困難になる。

【０１５１】

なお、図４１で説明したパーソナルコンピュータ１がアダプタ７に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対しステップＳ６５１に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

【０１５２】

最後に、パーソナルコンピュータ１がＥＭＤサーバ５から、事前に無料でダウンロードした音楽データを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図４４のフローチャートを参照して説明する。ステップＳ６７１において、パーソナルコンピュータ１は、インターネット４を介して、ＥＭＤサーバ５と相互認証する。ステップＳ６７２において、パーソナルコンピュータ１のＣＰＵ１２は、インターネット接続インターフェース１１を介して、ＥＭＤサーバ５に、音楽データの再生条件を示すデータを送信する。ステップＳ６７３において、ＥＭＤサーバ５は、受信した再生条件を示すデータを基に、支払い金額のデータをパーソナルコンピュータ１に送信する。

【０１５３】

ステップＳ６７４において、パーソナルコンピュータ１のＣＰＵ１２は、ＥＭＤサーバ５から受信した支払い金額のデータをディスプレイ３に表示させる。ステップＳ６７５において、ＥＭＤサーバ５は、パーソナルコンピュータ１に、ユーザのクレジットカードの番号等の送信を要求する。ステップＳ６７６において、ユーザは、入力部２を操作し、パーソナルコンピュータ１にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ１は、クレジットカードの番号等のデータをＥＭＤサーバ５に送信する。

【０１５４】

ステップＳ６７７において、ＥＭＤサーバ５は、パーソナルコンピュータ１から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。

ステップＳ６７８において、ＥＭＤサーバ５は、インターネット４を介して、パーソナルコンピュータ１に所定の暗号鍵を送信する。ステップＳ６７９において、パーソナルコンピュータ１は、インターネット４を介して、ＥＭＤサーバ５から送信された所定の暗号鍵を受信し、処理は終了する。

【０１５５】

以上のように、パーソナルコンピュータ１がＥＭＤサーバ５から暗号鍵をダウンロードするとともに、ＥＭＤサーバ５は、決済の処理をすれば、パーソナルコンピュータ１がＥＭＤサーバ５から音楽データをダウンロードするとき、認証、暗号化、または決済などの処理が必要なくなるので、比較的大きなデータである音楽データを迅速にダウンロードすることができる。

【０１５６】

以上においては、記録媒体として、メモリスティックウォークマン６を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行するとして説明したが、ｓｍａｓｈ（商標）などの手続きにより、決済をするようにしてもよい。

【０１５７】

また、図４４のフローチャートに示す処理の前に、パーソナルコンピュータ１とＥＭＤサーバ５とが、例えば、IS09798-3で規定されているhttp(Hypertext Transport Protocol)上のプロトコルを使用して、相互認証するようにしてもよい。

【０１５８】

なお、メモリスティックウォークマン６は、予め個別鍵を記憶しているして説明したが、ユーザがメモリスティックウォークマン６を購入後、ＥＭＤサーバ５などからダウンロードするようにしてもよい。

【０１５９】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【０１６０】

以上のように、本発明によれば、次のような効果を奏することができる。

【０１６１】

（１）　ハードディスク１５に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でハードディスク１５に記録するようにしたので、ハードディスク１５に記録されている音楽データをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【０１６２】

（２）　所定の曲を１回コピーしたとき、一定時間（上記例の場合、４８時間）の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【０１６３】

さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【０１６４】

（３）　外部の装置に音楽データを渡したら、ハードディスク１５上の音楽データを消去するようにしたので、ハードディスク１５内に元のデジタル音楽データが残らず、その複製を大量に配布することが防止される。

【０１６５】

（４）　ハードディスク１５内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、ハードディスク１５の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをハードディスク１５にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【０１６６】

（５）　パーソナルコンピュータ１が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【０１６７】

（６）　外部機器から、パーソナルコンピュータ１に対してデータを渡す前に、パーソナルコンピュータ１のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対して音楽データを渡してしまうようなことが防止される。

【０１６８】

（７）　曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【０１６９】

（８）　パーソナルコンピュータ１におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ１に外付けされるアダプタ７に負担させるようにしたので、パーソナルコンピュータ１のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【０１７０】

更に、そのソフトウェアが、安全な認証局またはＥＭＤサーバ５で暗号化またはシャッフルされるので、ソフトウェアの改竄は、より困難となる。

【０１７１】

（９）　プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ７が生成する固有の鍵で暗号化するようにしたので、プログラムのみをＣＤ－ＲＯＭなどの媒体で配布可能にしつつ、プログラムを他のアダプタ７で実行することが防止される。

【０１７２】

（１０）　音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

【０１７３】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０１７４】

なお、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０１７５】

【発明の効果】

請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載の提供媒体によれば、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【０１７６】

請求項６に記載の情報処理システムによれば、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信され、半導体ＩＣに実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【図面の簡単な説明】

【図１】

本発明を適用したシステムの構成例を示すブロック図である。

【図２】

図１のシステムにおいてコンパクトディスクからハードディスク１５にコピーする場合の処理を説明するフローチャートである。

【図３】

図２のステップＳ１２の期限データベースチェック処理を説明するフローチャートである。

【図４】

期限データベースの例を示す図である。

【図５】

ウォータマークを説明する図である。

【図６】

曲データベースの例を示す図である。

【図７】

図１のシステムのハードディスク１５からメモリスティックウォークマン６へデータを移動する動作を説明するフローチャートである。

【図８】

図１のシステムのハードディスク１５からメモリスティックウォークマン６へデータを移動する動作を説明するフローチャートである。

【図９】

図１のシステムのハードディスク１５からメモリスティックウォークマン６へデータを移動する作を説明するフローチャートである。

【図１０】

図７のステップＳ５５の選択曲の再生条件などのチェック処理を説明するフローチャートである。

【図１１】

メモリスティックウォークマンが管理している再生条件を説明する図である。

【図１２】

図７のステップＳ５８のフォーマット変換処理の詳細を説明するフローチャートである。

【図１３】

図１のハードディスク１５からメモリスティックウォークマン６へデータをコピーする場合の動作を説明するフローチャートである。

【図１４】

図１のハードディスク１５からメモリスティックウォークマン６へデータをコピーする場合の動作を説明するフローチャートである。

【図１５】

図１のハードディスク１５からメモリスティックウォークマン６へデータをコピーする場合の動作を説明するフローチャートである。

【図１６】

図１のメモリスティックウォークマン６からハードディスク１５へデータを移動する場合の動作を説明するフローチャートである。

【図１７】

図１のシステムのメモリスティックウォークマン６からハードディスク１５へデータをコピーする場合の動作を説明フローチャートである。

【図１８】

図１のシステムのEMDサーバ５からハードディスク１５へデータをコピーする場合の処理を説明するフローチャートである。

【図１９】

図１８のステップＳ２０４の課金に関する処理の詳細を説明するフローチャートである。

【図２０】

課金ログを説明する図である。

【図２１】

図１のシステムのIEC６０９５８端子１６ａからハードディスク１５へデータをコピーする２合の処理を説明するフローチャートである。

【図２２】

図１のシステムのIEC６０９５８端子１６ａからハードディスク１５へデータをコピーする場合の処理を説明するフローチャートである。

【図２３】

図１のシステムのハードディスク１５からIEC６０９５８端子１６ａにデータを出力する場合の動作を説明するフローチャートである。

【図２４】

図１のシステムのハードディスク１５からIEC６０９５８端子１６ａにデータを出力する場合の動作を説明するフローチャートである。

【図２５】

図２３のステップＳ２７５の再生条件などのチェック処理を説明するフローチャートである。

【図２６】

図１のシステムのハードディスク１５からメモリスティックウォークマン６経由でデータを出力する場合の動作を説明するフローチャートである。

【図２７】

図１のシステムのハードディスク１５からメモリスティックウォークマン６経由でデータを出力する場合の動作を説明するフローチャートである。

【図２８】

図１の不揮発性メモリ３４の機能を説明する図である。

【図２９】

図１のシステムのアダプタ７の動作を説明するフローチャートである。

【図３０】

図１のシステムのアダプタ７の内部の構成を示す図である。

【図３１】

図３１の不揮発性メモリ３４の内部の構成例を示す図である。

【図３２】

図３１の不揮発性メモリ３４の内部の構成例を示す図である。

【図３３】

アダプタ７とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図３４】

アダプタ７とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図３５】

アダプタ７とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図３６】

アダプタ７とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図３７】

ソースプログラムを暗号化する処理を説明するフローチャートである。

【図３８】

暗号化されたソースプログラムをアダプタ７が実行する処理を説明するフローチャートである。

【図３９】

オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

【図４０】

暗号化されたオブジェクトプログラムをアダプタ７が実行する処理を説明するフローチャートである。

【図４１】

オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

【図４２】

暗号化されたオブジェクトプログラムをアダプタ７が実行する他の処理を説明するフローチャートである。

【図４３】

アダプタ７がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ１のＣＰＵ１２に実行させるときの処理を説明するフローチャートである。

【図４４】

パーソナルコンピュータ１がＥＭＤサーバ５から暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

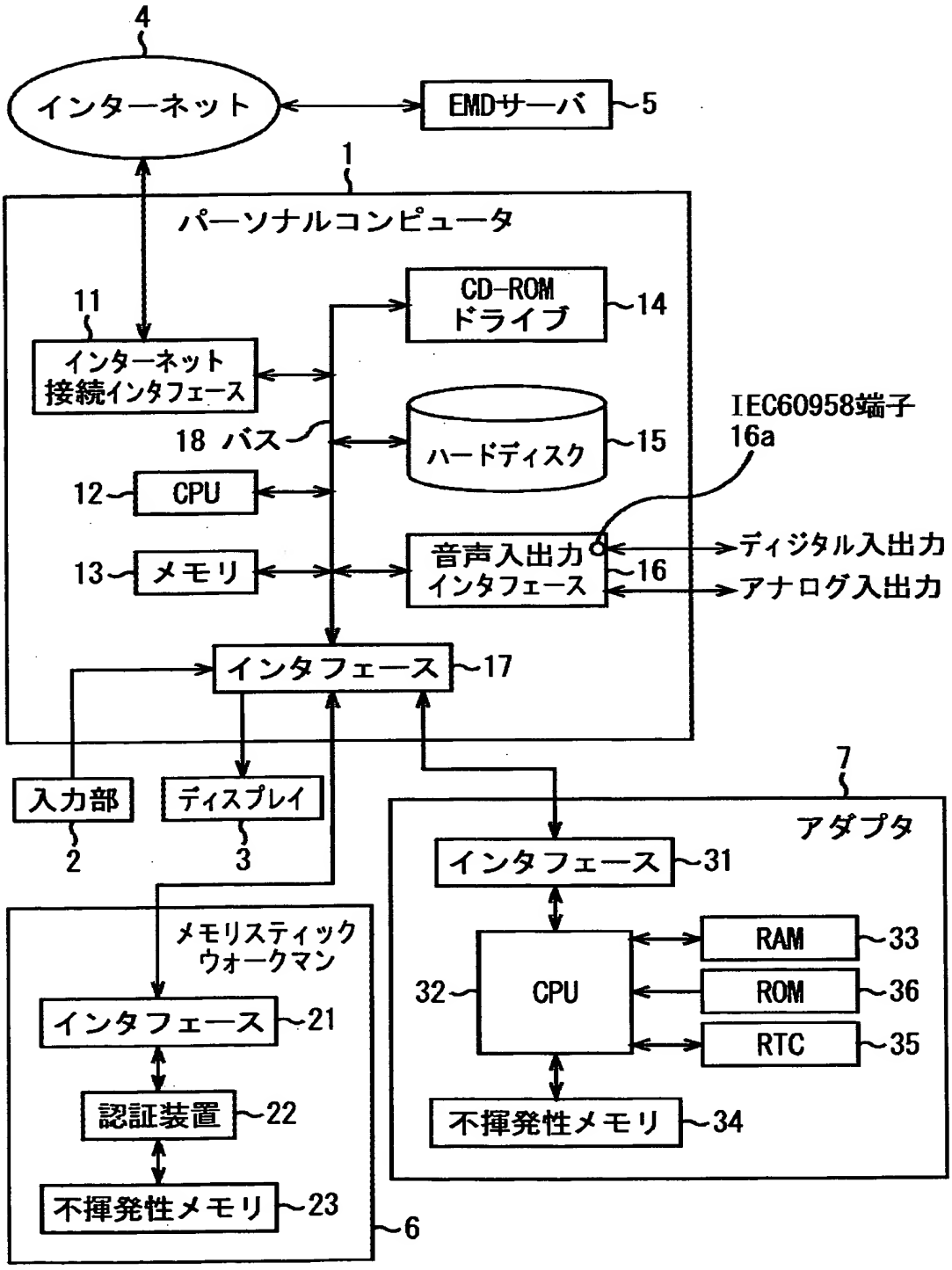
【符号の説明】

１　パーソナルコンピュータ，　２　入力部，　３　ディスプレイ，　４　インターネット，　５　EMDサーバ，　６　メモリスティックウォークマン，　７　アダプタ，　１２　CPU，　１３　メモリ，　１４　CD-ROMドライブ，　１５

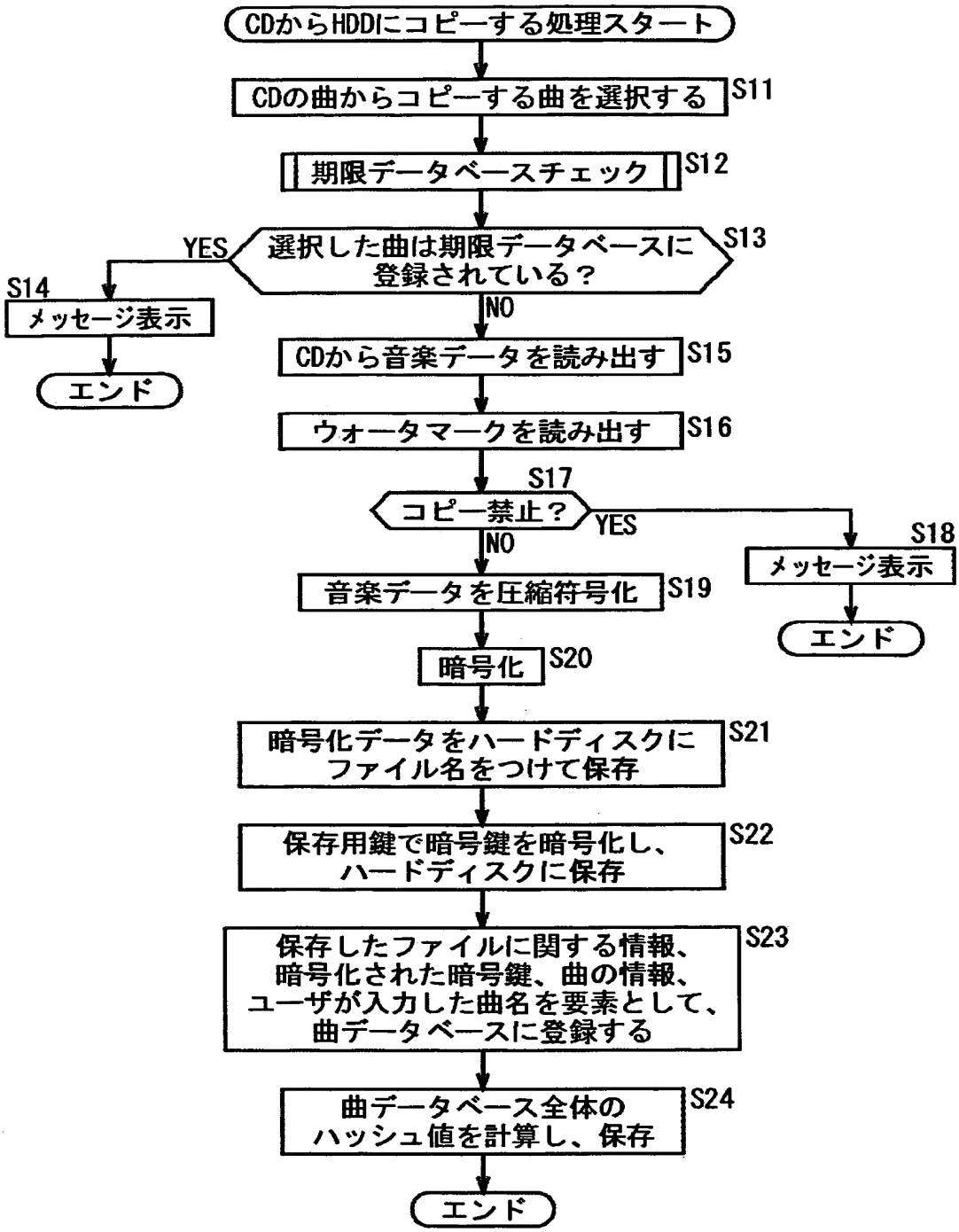
ハードディスク，　１６　音声入出力インタフェース，　１６ａ　IEC６０９５８端子，　２２　認証装置，　２３　不揮発性メモリ，　３２　CPU

【書類名】図面

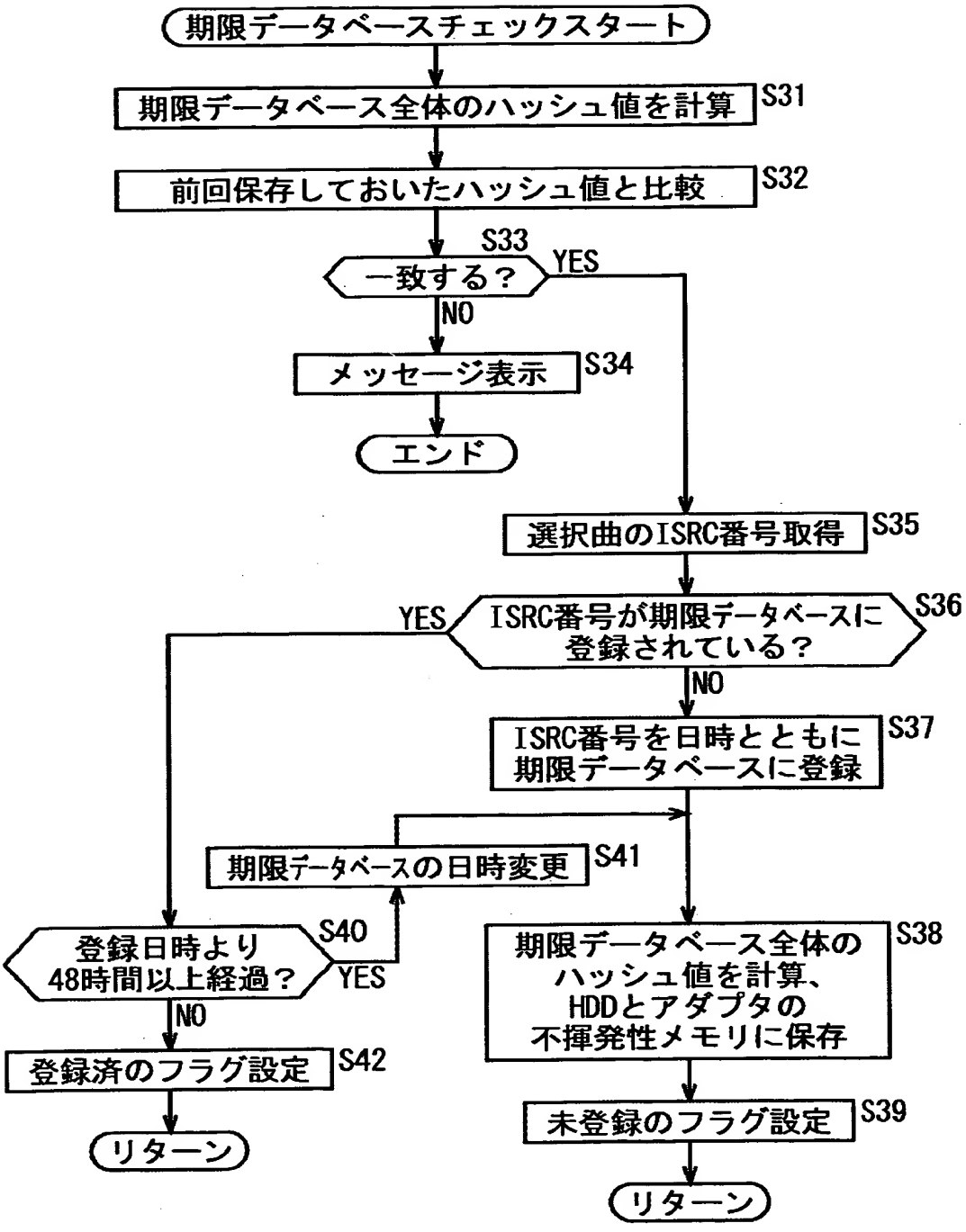
【図１】


4
インターネット
EMDサーバ
5
1
パーソナルコンピュータ
11
インターネット
接続インタフェース
CD-ROM
ドライブ
14
18 バス
ハードディスク
15
IEC60958端子
16a
12
CPU
13
メモリ
音声入出力
インタフェース
16
ディジタル入出力
アナログ入出力
インタフェース
17
入力部
2
ディスプレイ
3
7
アダプタ
インタフェース
31
RAM
33
32
CPU
ROM
36
RTC
35
不揮発性メモリ
34
メモリスティック
ウォークマン
インタフェース
21
認証装置
22
不揮発性メモリ
23
6

【図２】


CDからHDDにコピーする処理スタート
CDの曲からコピーする曲を選択する
S11
期限データベースチェック
S12
選択した曲は期限データベースに登録されている？
S13
YES
S14
メッセージ表示
エンド
NO
CDから音楽データを読み出す
S15
ウォータマークを読み出す
S16
S17
コピー禁止？
YES
S18
メッセージ表示
エンド
NO
音楽データを圧縮符号化
S19
暗号化
S20
暗号化データをハードディスクにファイル名をつけて保存
S21
保存用鍵で暗号鍵を暗号化し、ハードディスクに保存
S22
保存したファイルに関する情報、暗号化された暗号鍵、曲の情報、ユーザが入力した曲名を要素として、曲データベースに登録する
S23
曲データベース全体のハッシュ値を計算し、保存
S24
エンド

【図３】


期限データベースチェックスタート
期限データベース全体のハッシュ値を計算
S31
前回保存しておいたハッシュ値と比較
S32
S33
一致する？
YES
NO
メッセージ表示
S34
エンド
選択曲のISRC番号取得
S35
YES
ISRC番号が期限データベースに登録されている？
S36
NO
ISRC番号を日時とともに期限データベースに登録
S37
期限データベースの日時変更
S41
登録日時より48時間以上経過？
S40
YES
NO
登録済のフラグ設定
S42
リターン
期限データベース全体のハッシュ値を計算、HDDとアダプタの不揮発性メモリに保存
S38
未登録のフラグ設定
S39
リターン

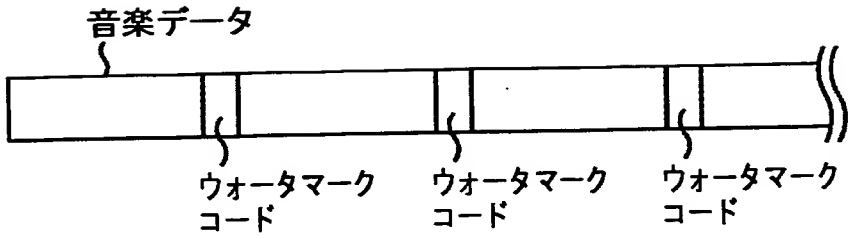
【図４】

期限データベース

	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934

【図５】



【図６】

曲データベース

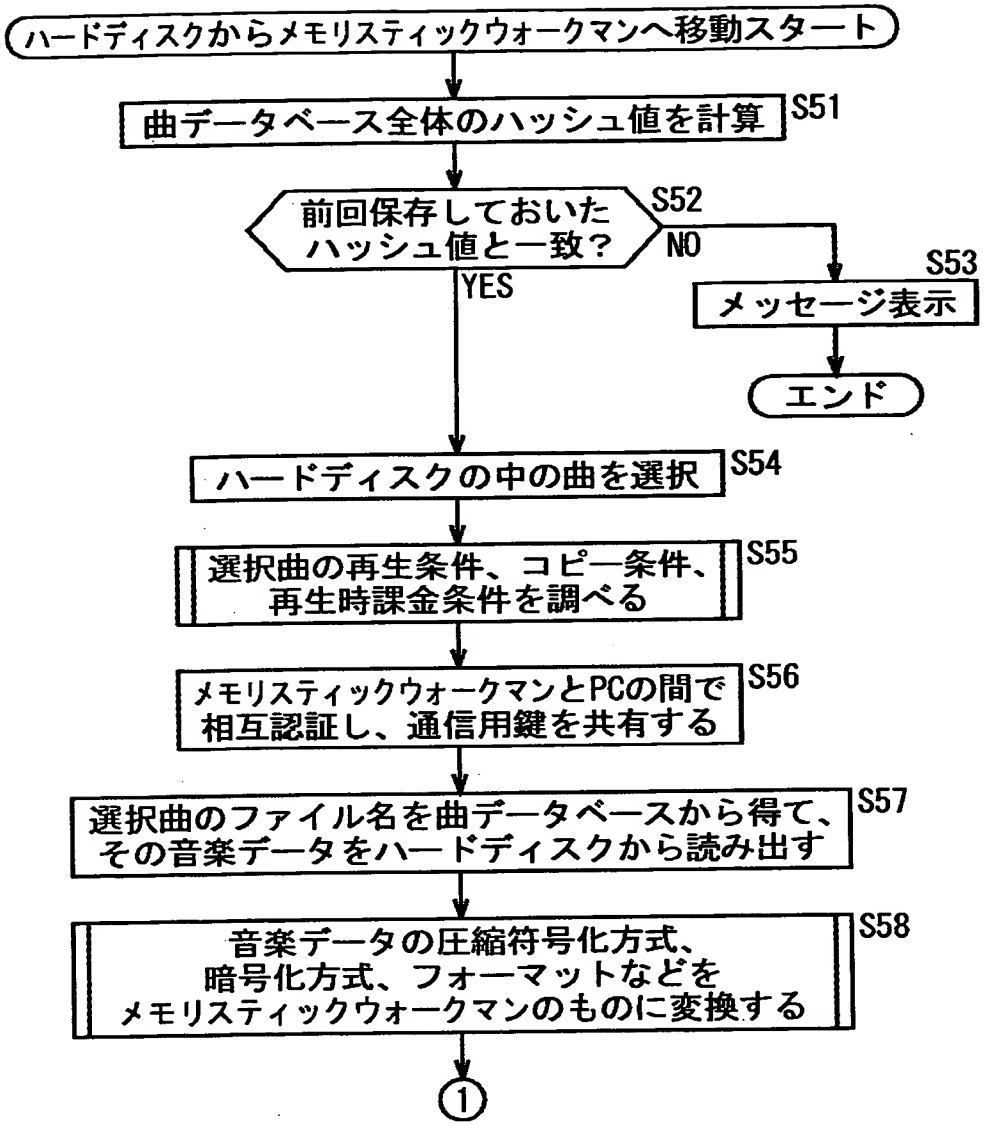
	アイテム1	アイテム2	アイテム3	
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2	
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件:開始日時	-	2001.01.01.00:00	-	
再生条件:終了日時	1999.07.31.23:59	-	-	
再生条件:回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	¥5	
コピー条件:回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件:SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321

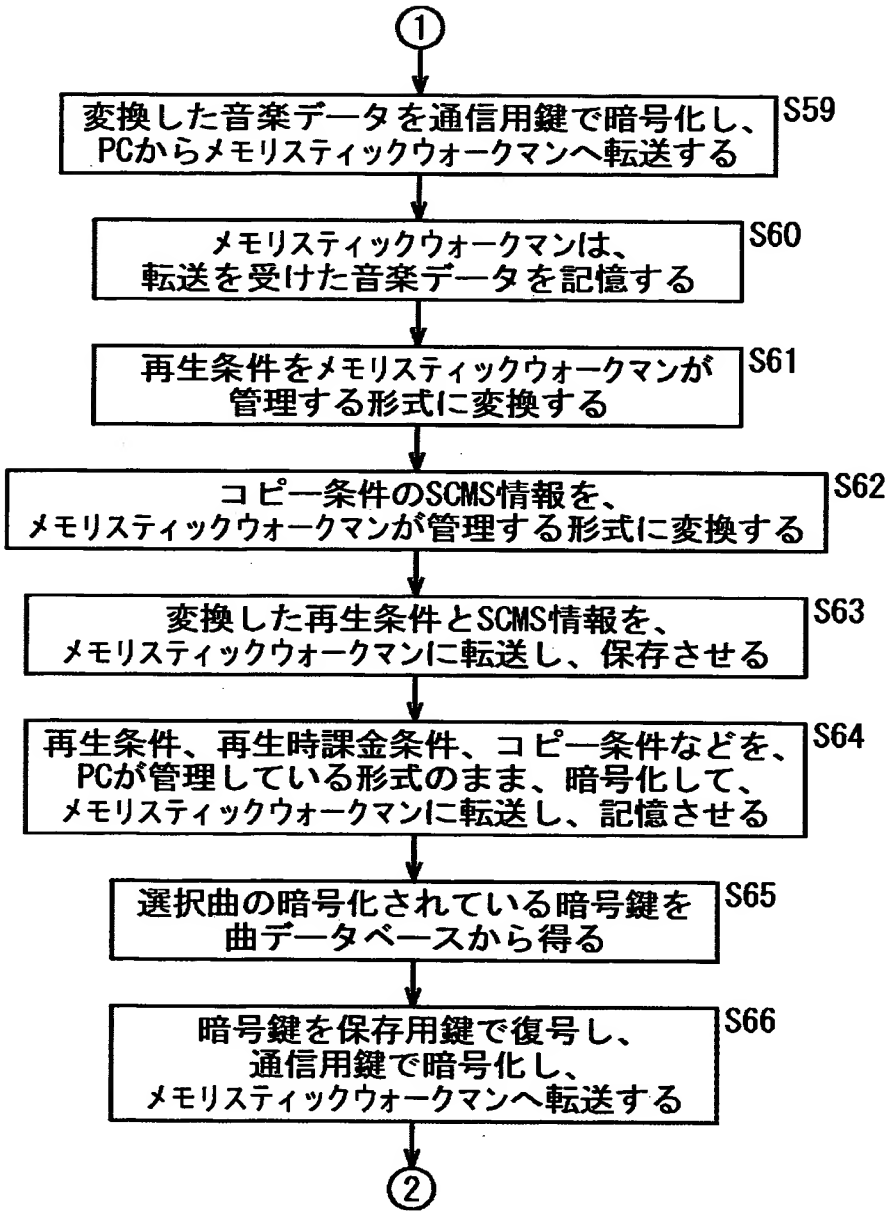
特平１１－０８８３４６

出証特２０００－３００１０４

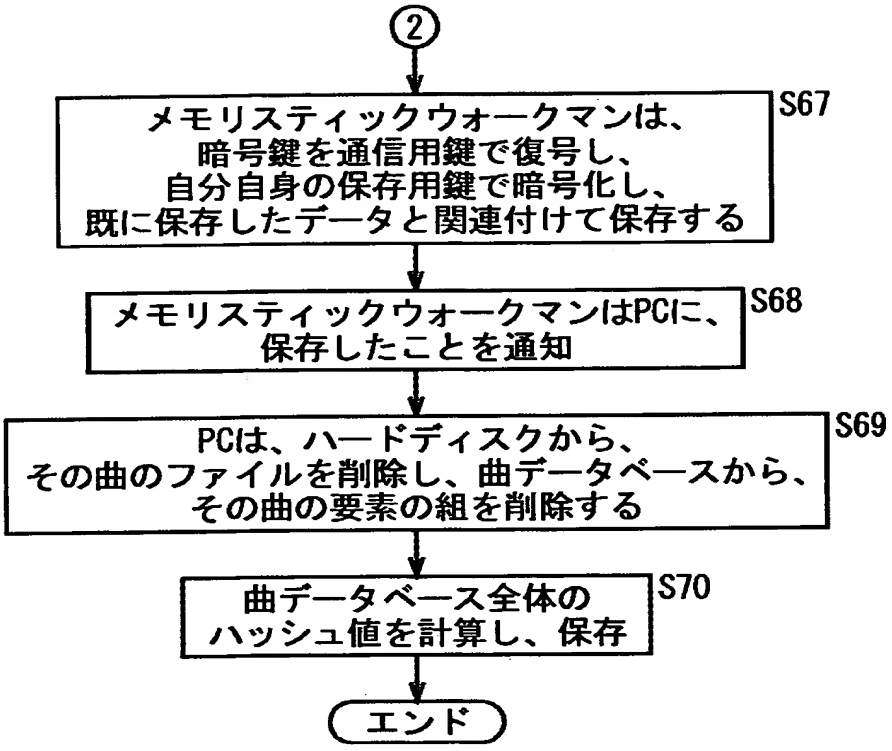
【図７】


ハードディスクからメモリスティックウォークマンへ移動スタート
曲データベース全体のハッシュ値を計算
S51
前回保存しておいた
ハッシュ値と一致？
S52
NO
YES
S53
メッセージ表示
エンド
ハードディスクの中の曲を選択
S54
選択曲の再生条件、コピー条件、
再生時課金条件を調べる
S55
メモリスティックウォークマンとPCの間で
相互認証し、通信用鍵を共有する
S56
選択曲のファイル名を曲データベースから得て、
その音楽データをハードディスクから読み出す
S57
音楽データの圧縮符号化方式、
暗号化方式、フォーマットなどを
メモリスティックウォークマンのものに変換する
S58
①

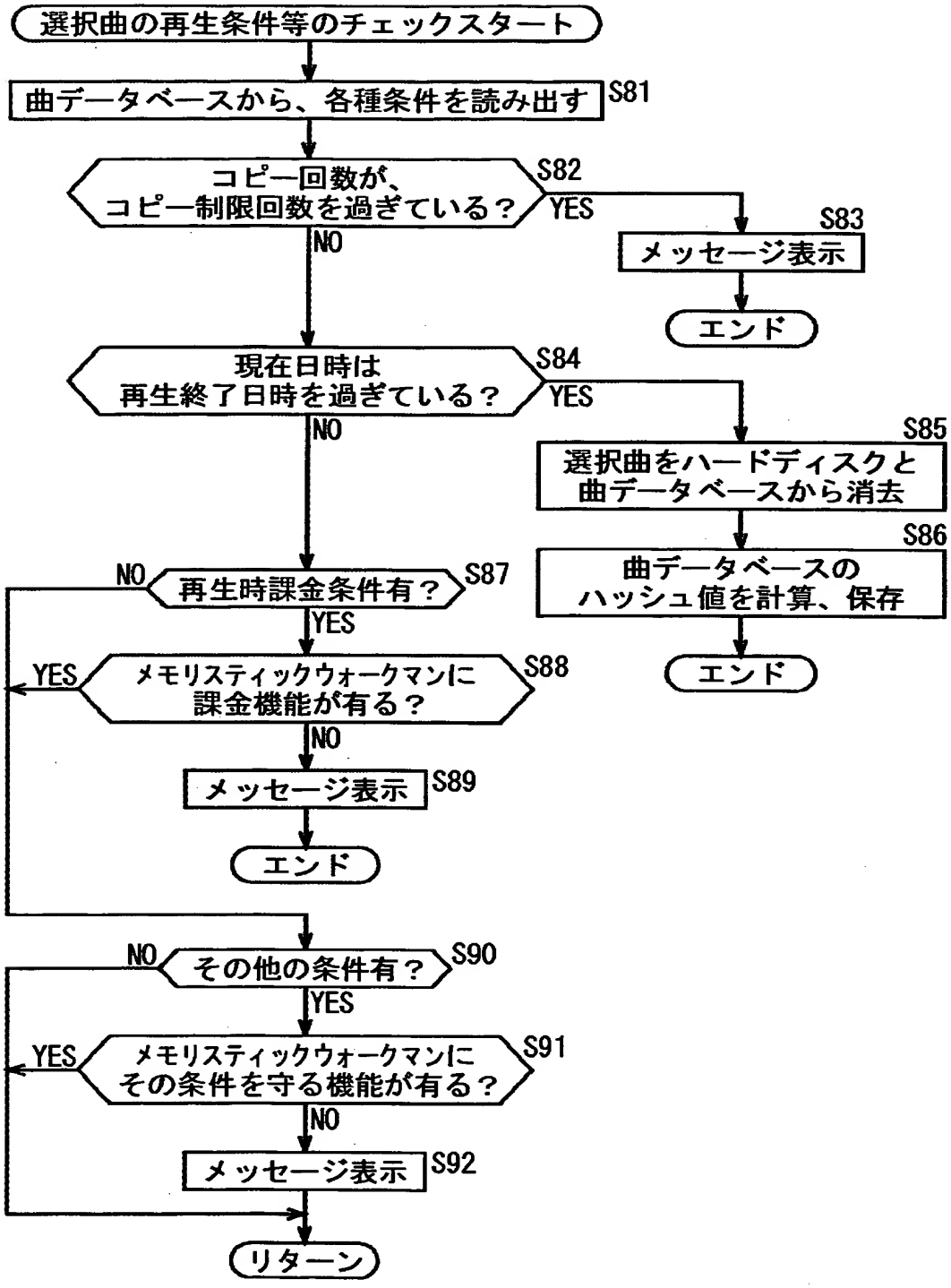
【図８】


①
変換した音楽データを通信用鍵で暗号化し、PCからメモリスティックウォークマンへ転送する
S59
メモリスティックウォークマンは、転送を受けた音楽データを記憶する
S60
再生条件をメモリスティックウォークマンが管理する形式に変換する
S61
コピー条件のSCMS情報を、メモリスティックウォークマンが管理する形式に変換する
S62
変換した再生条件とSCMS情報を、メモリスティックウォークマンに転送し、保存させる
S63
再生条件、再生時課金条件、コピー条件などを、PCが管理している形式のまま、暗号化して、メモリスティックウォークマンに転送し、記憶させる
S64
選択曲の暗号化されている暗号鍵を曲データベースから得る
S65
暗号鍵を保存用鍵で復号し、通信用鍵で暗号化し、メモリスティックウォークマンへ転送する
S66
②

【図９】


②
メモリスティックウォークマンは、
暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化し、
既に保存したデータと関連付けて保存する
S67
メモリスティックウォークマンはPCに、
保存したことを通知
S68
PCは、ハードディスクから、
その曲のファイルを削除し、曲データベースから、
その曲の要素の組を削除する
S69
曲データベース全体の
ハッシュ値を計算し、保存
S70
エンド

【図１０】

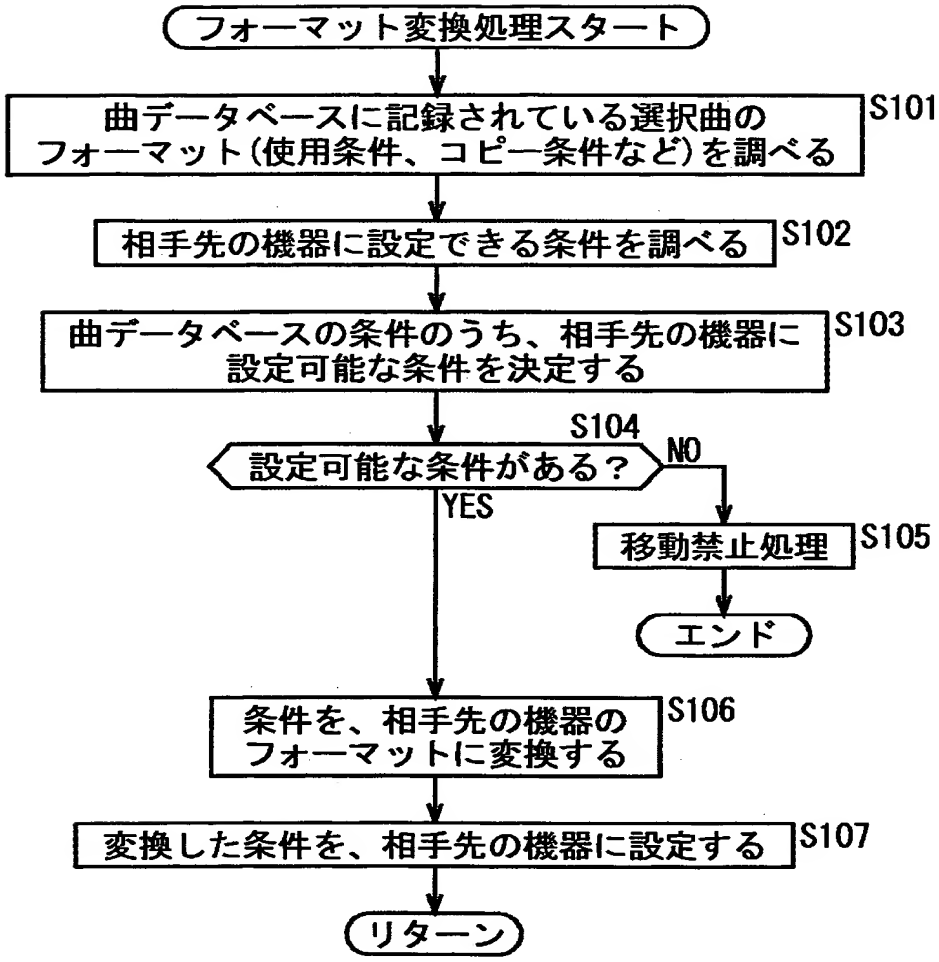

選択曲の再生条件等のチェックスタート
曲データベースから、各種条件を読み出す
S81
コピー回数が、
コピー制限回数を過ぎている？
S82
YES
NO
S83
メッセージ表示
エンド
現在日時は
再生終了日時を過ぎている？
S84
YES
NO
S85
選択曲をハードディスクと
曲データベースから消去
S86
曲データベースの
ハッシュ値を計算、保存
エンド
NO
再生時課金条件有？
S87
YES
YES
メモリスティックウォークマンに
課金機能が有る？
S88
NO
メッセージ表示
S89
エンド
NO
その他の条件有？
S90
YES
YES
メモリスティックウォークマンに
その条件を守る機能が有る？
S91
NO
メッセージ表示
S92
リターン

【図１１】

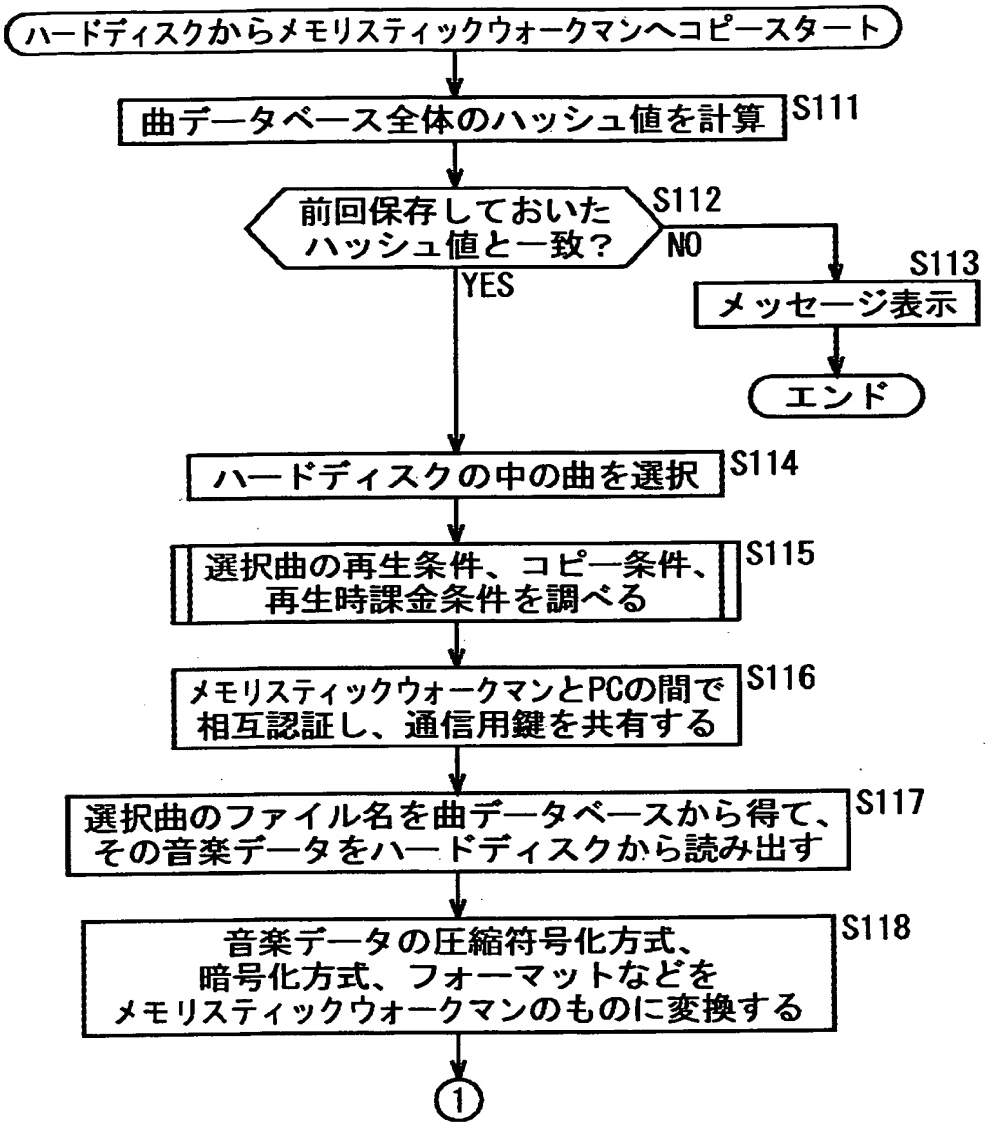
メモリスティックウォークマンが管理している再生条件

	アイテム1	アイテム2	アイテム3
曲ID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

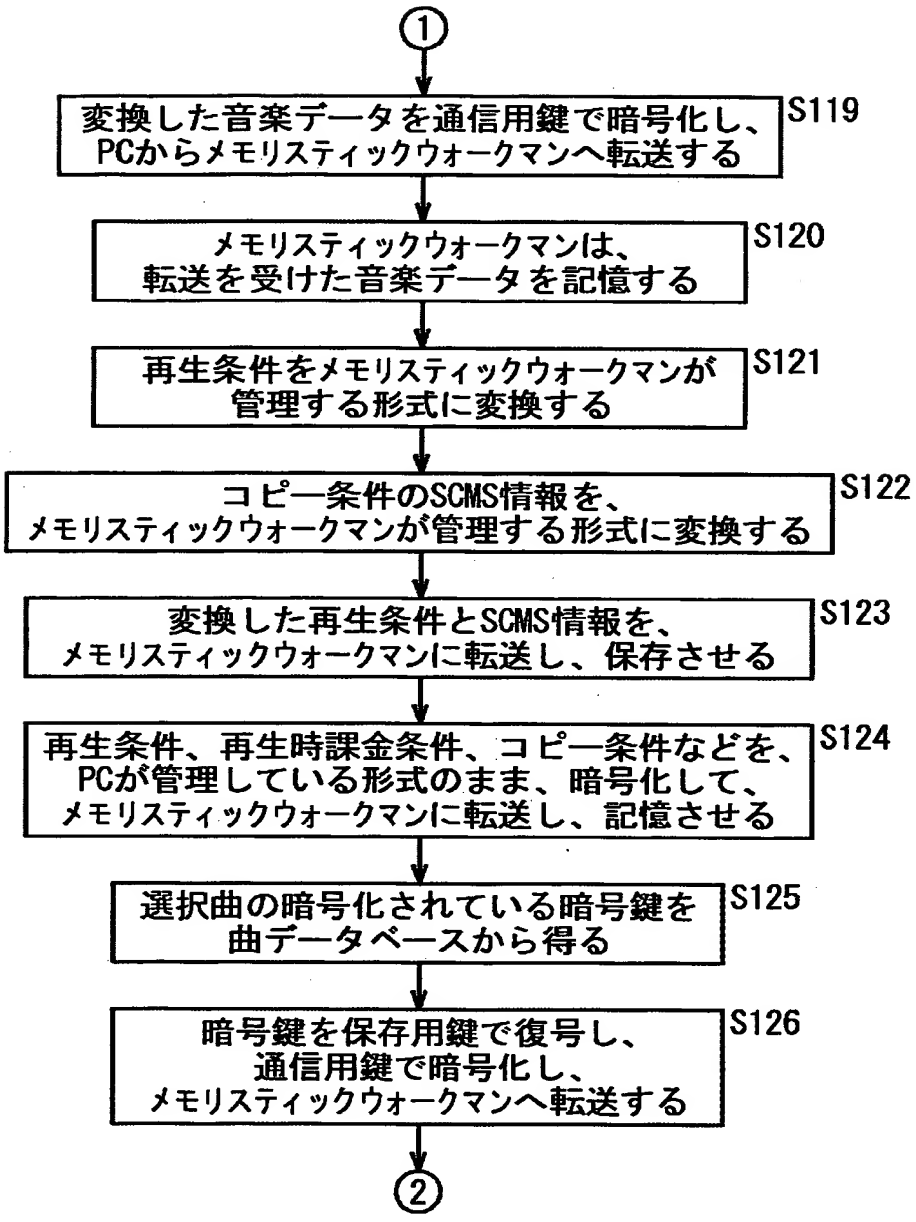
【図１２】


フォーマット変換処理スタート
曲データベースに記録されている選択曲のフォーマット(使用条件、コピー条件など)を調べる
S101
相手先の機器に設定できる条件を調べる
S102
曲データベースの条件のうち、相手先の機器に設定可能な条件を決定する
S103
S104
設定可能な条件がある？
NO
YES
移動禁止処理
S105
エンド
条件を、相手先の機器のフォーマットに変換する
S106
変換した条件を、相手先の機器に設定する
S107
リターン

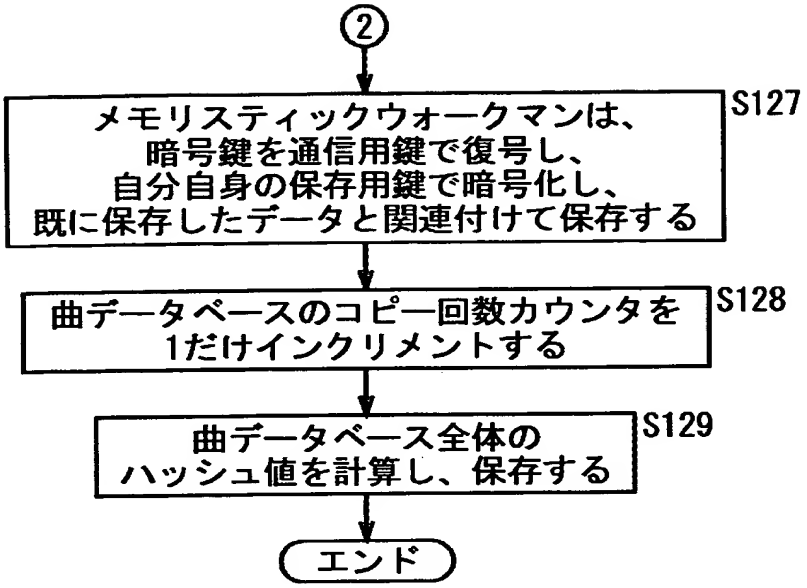
【図１３】


ハードディスクからメモリスティックウォークマンへコピースタート
曲データベース全体のハッシュ値を計算
S111
前回保存しておいた
ハッシュ値と一致？
S112
NO
YES
S113
メッセージ表示
エンド
ハードディスクの中の曲を選択
S114
選択曲の再生条件、コピー条件、
再生時課金条件を調べる
S115
メモリスティックウォークマンとPCの間で
相互認証し、通信用鍵を共有する
S116
選択曲のファイル名を曲データベースから得て、
その音楽データをハードディスクから読み出す
S117
音楽データの圧縮符号化方式、
暗号化方式、フォーマットなどを
メモリスティックウォークマンのものに変換する
S118
①

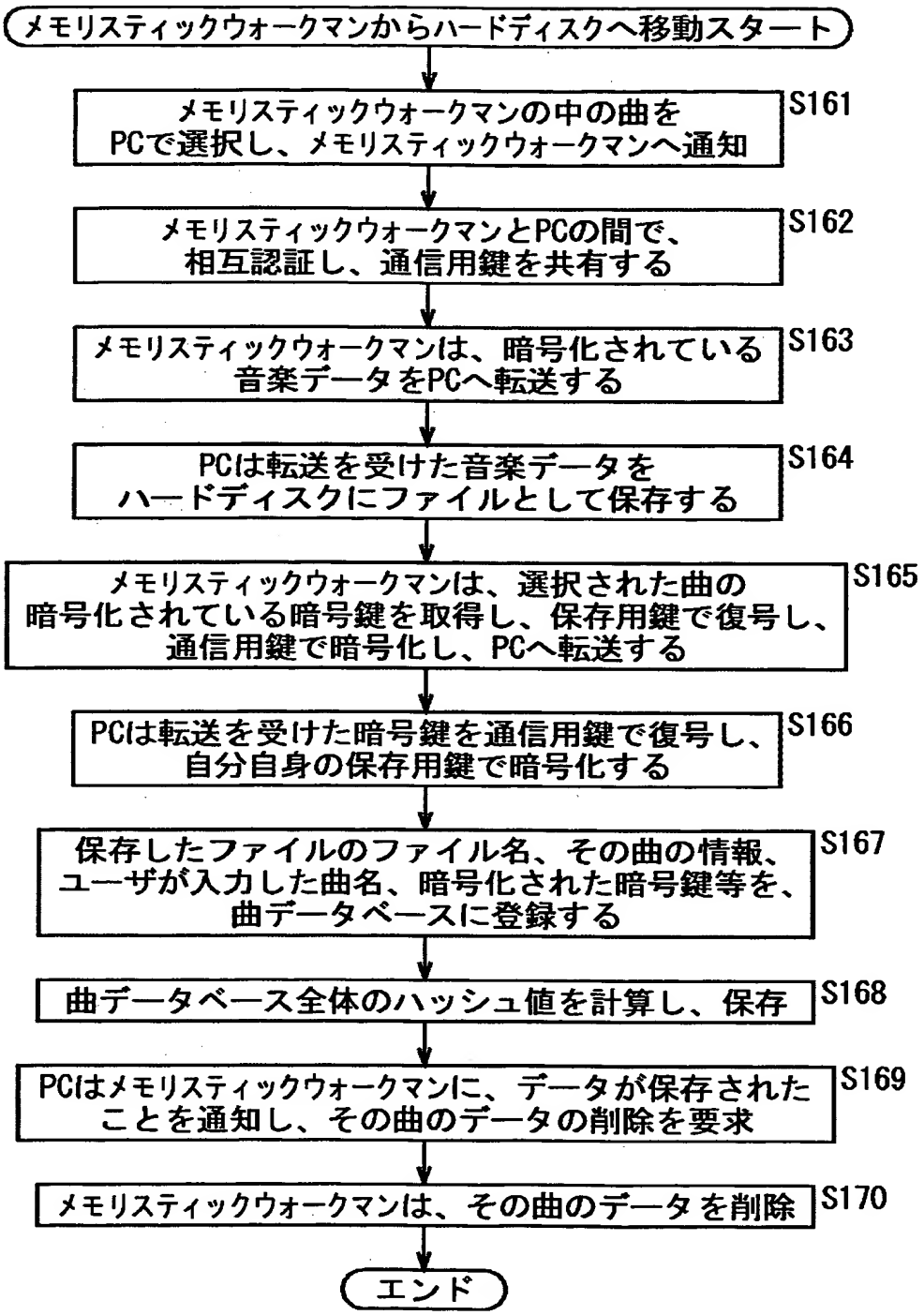
【図１４】


①
変換した音楽データを通信用鍵で暗号化し、PCからメモリスティックウォークマンへ転送する
S119
メモリスティックウォークマンは、転送を受けた音楽データを記憶する
S120
再生条件をメモリスティックウォークマンが管理する形式に変換する
S121
コピー条件のSCMS情報を、メモリスティックウォークマンが管理する形式に変換する
S122
変換した再生条件とSCMS情報を、メモリスティックウォークマンに転送し、保存させる
S123
再生条件、再生時課金条件、コピー条件などを、PCが管理している形式のまま、暗号化して、メモリスティックウォークマンに転送し、記憶させる
S124
選択曲の暗号化されている暗号鍵を曲データベースから得る
S125
暗号鍵を保存用鍵で復号し、通信用鍵で暗号化し、メモリスティックウォークマンへ転送する
S126
②

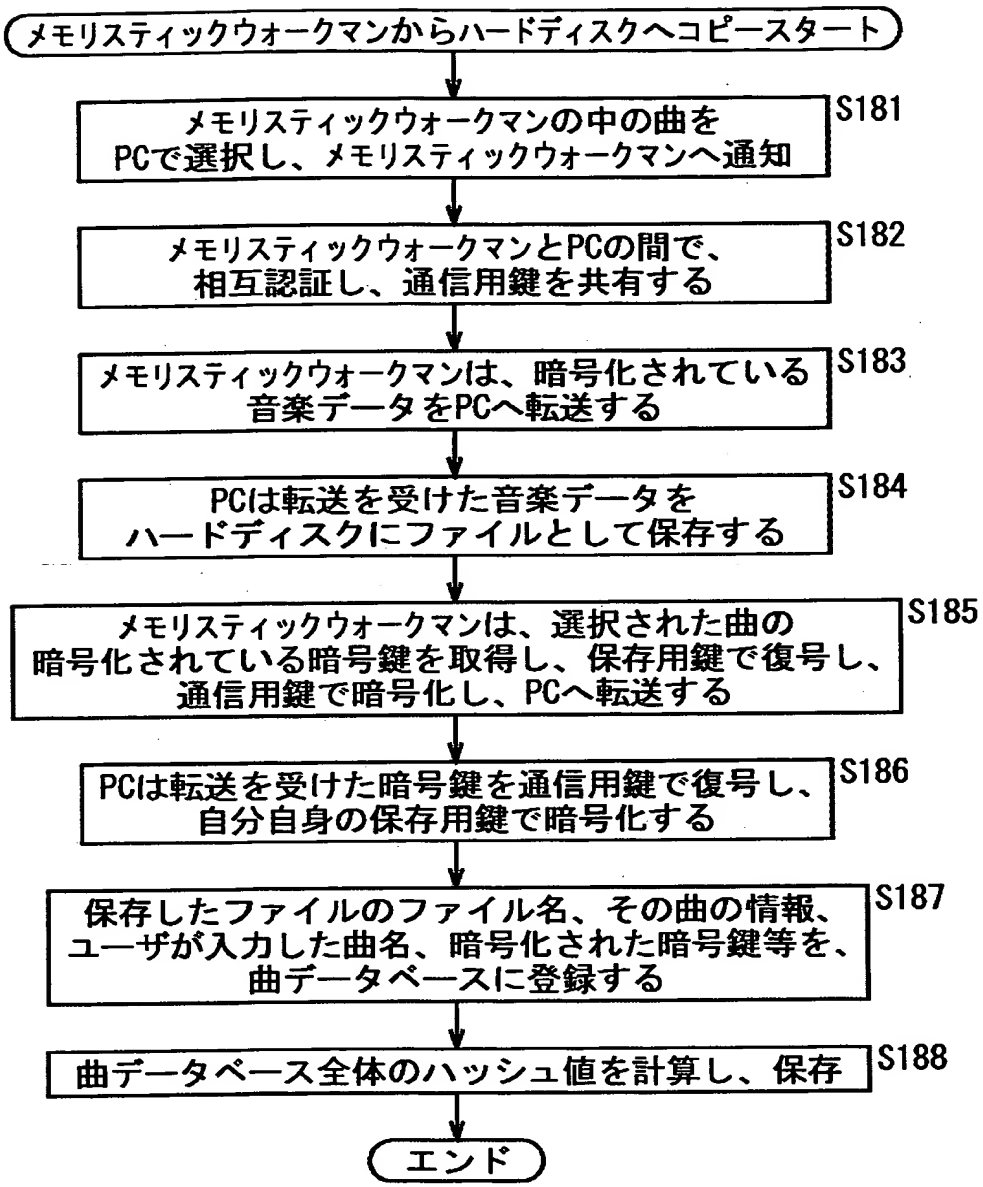
【図１５】


②
メモリスティックウォークマンは、
暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化し、
既に保存したデータと関連付けて保存する
S127
曲データベースのコピー回数カウンタを
1だけインクリメントする
S128
曲データベース全体の
ハッシュ値を計算し、保存する
S129
エンド

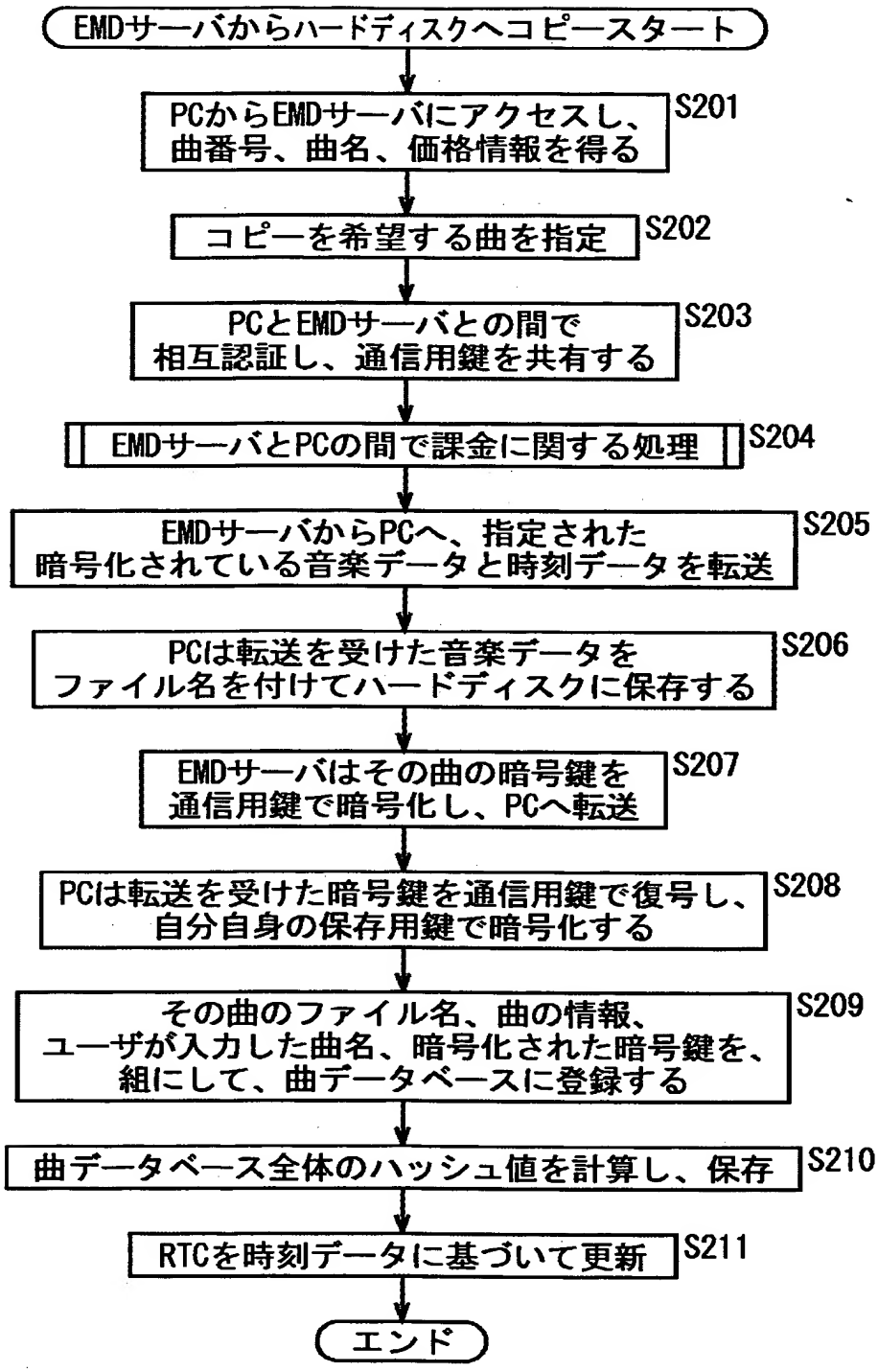
【図１６】


メモリスティックウォークマンからハードディスクへ移動スタート
メモリスティックウォークマンの中の曲を
PCで選択し、メモリスティックウォークマンへ通知
S161
メモリスティックウォークマンとPCの間で、
相互認証し、通信用鍵を共有する
S162
メモリスティックウォークマンは、暗号化されている
音楽データをPCへ転送する
S163
PCは転送を受けた音楽データを
ハードディスクにファイルとして保存する
S164
メモリスティックウォークマンは、選択された曲の
暗号化されている暗号鍵を取得し、保存用鍵で復号し、
通信用鍵で暗号化し、PCへ転送する
S165
PCは転送を受けた暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化する
S166
保存したファイルのファイル名、その曲の情報、
ユーザが入力した曲名、暗号化された暗号鍵等を、
曲データベースに登録する
S167
曲データベース全体のハッシュ値を計算し、保存
S168
PCはメモリスティックウォークマンに、データが保存された
ことを通知し、その曲のデータの削除を要求
S169
メモリスティックウォークマンは、その曲のデータを削除
S170
エンド

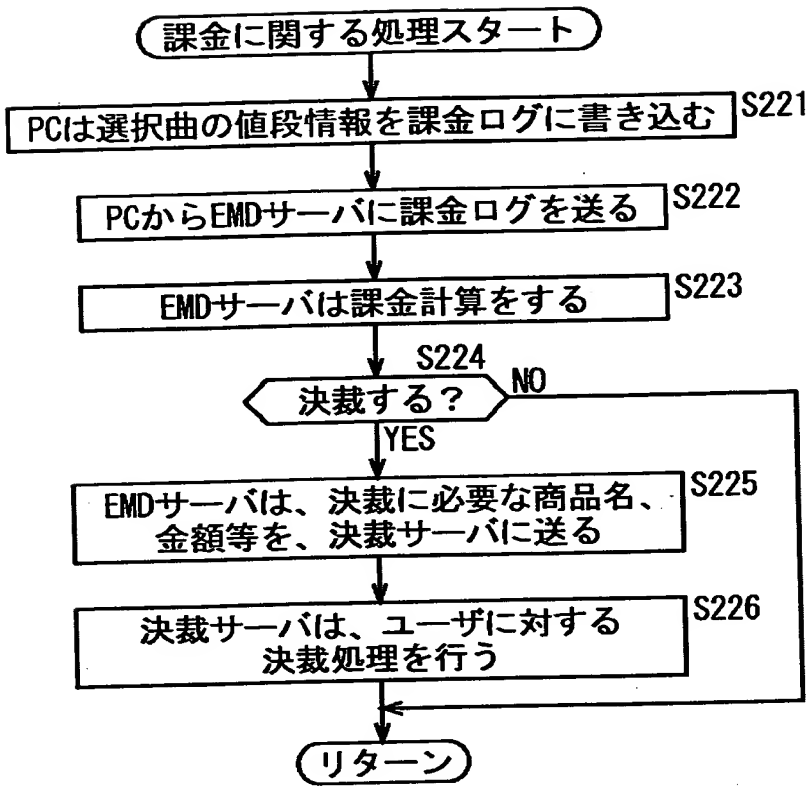
【図１７】


メモリスティックウォークマンからハードディスクへコピースタート
メモリスティックウォークマンの中の曲を
PCで選択し、メモリスティックウォークマンへ通知
S181
メモリスティックウォークマンとPCの間で、
相互認証し、通信用鍵を共有する
S182
メモリスティックウォークマンは、暗号化されている
音楽データをPCへ転送する
S183
PCは転送を受けた音楽データを
ハードディスクにファイルとして保存する
S184
メモリスティックウォークマンは、選択された曲の
暗号化されている暗号鍵を取得し、保存用鍵で復号し、
通信用鍵で暗号化し、PCへ転送する
S185
PCは転送を受けた暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化する
S186
保存したファイルのファイル名、その曲の情報、
ユーザが入力した曲名、暗号化された暗号鍵等を、
曲データベースに登録する
S187
曲データベース全体のハッシュ値を計算し、保存
S188
エンド

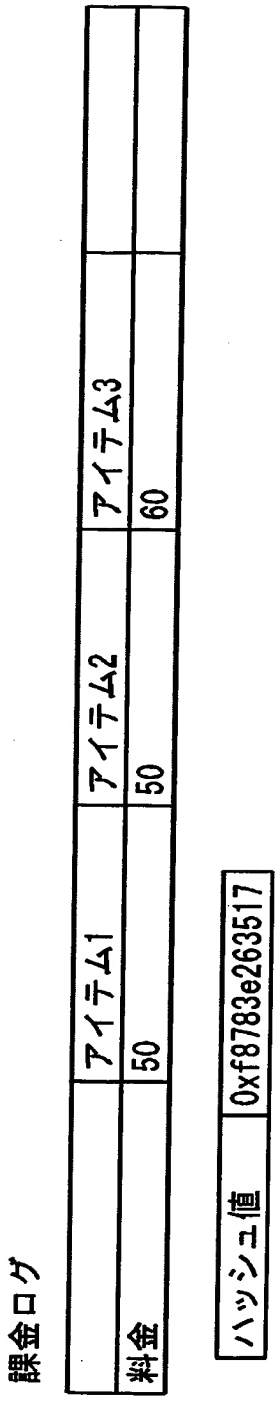
【図１８】


EMDサーバからハードディスクへコピースタート
PCからEMDサーバにアクセスし、曲番号、曲名、価格情報を得る
S201
コピーを希望する曲を指定
S202
PCとEMDサーバとの間で相互認証し、通信用鍵を共有する
S203
EMDサーバとPCの間で課金に関する処理
S204
EMDサーバからPCへ、指定された暗号化されている音楽データと時刻データを転送
S205
PCは転送を受けた音楽データをファイル名を付けてハードディスクに保存する
S206
EMDサーバはその曲の暗号鍵を通信用鍵で暗号化し、PCへ転送
S207
PCは転送を受けた暗号鍵を通信用鍵で復号し、自分自身の保存用鍵で暗号化する
S208
その曲のファイル名、曲の情報、ユーザが入力した曲名、暗号化された暗号鍵を、組にして、曲データベースに登録する
S209
曲データベース全体のハッシュ値を計算し、保存
S210
RTCを時刻データに基づいて更新
S211
エンド

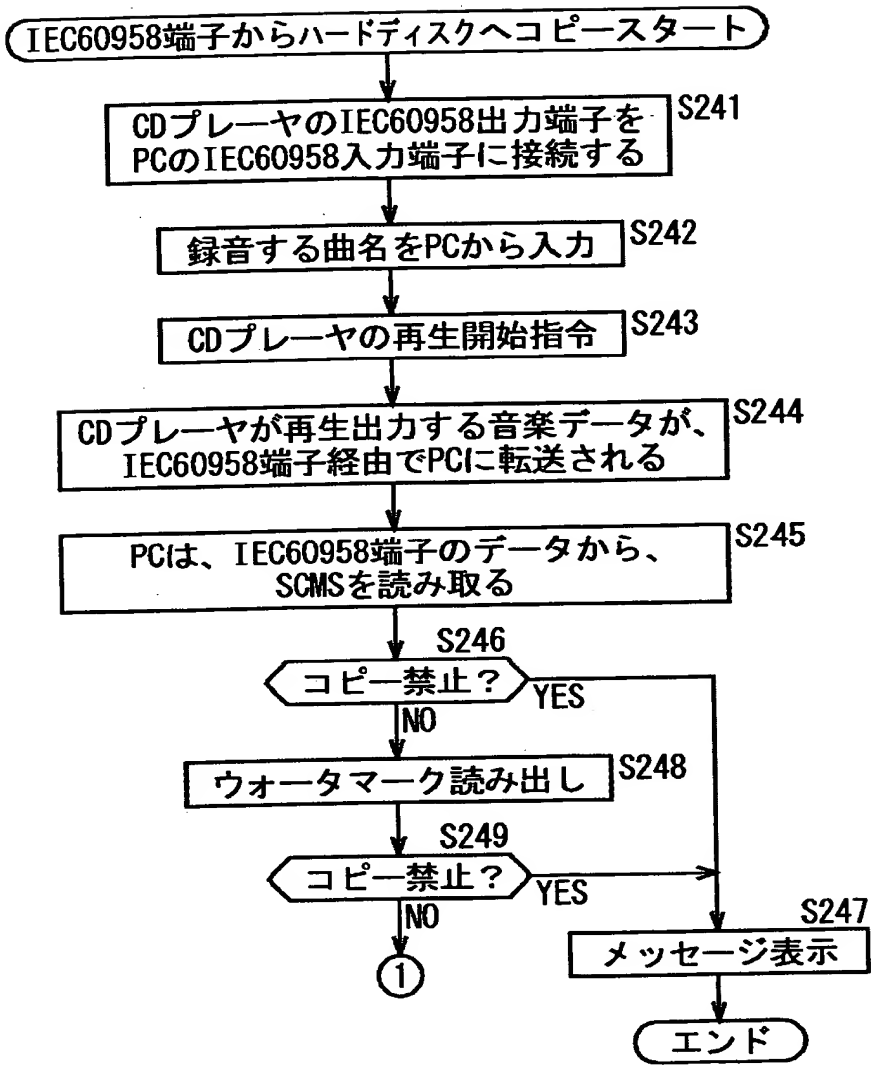
【図１９】


課金に関する処理スタート
PCは選択曲の値段情報を課金ログに書き込む
S221
PCからEMDサーバに課金ログを送る
S222
EMDサーバは課金計算をする
S223
S224
決裁する？
NO
YES
EMDサーバは、決裁に必要な商品名、
金額等を、決裁サーバに送る
S225
決裁サーバは、ユーザに対する
決裁処理を行う
S226
リターン

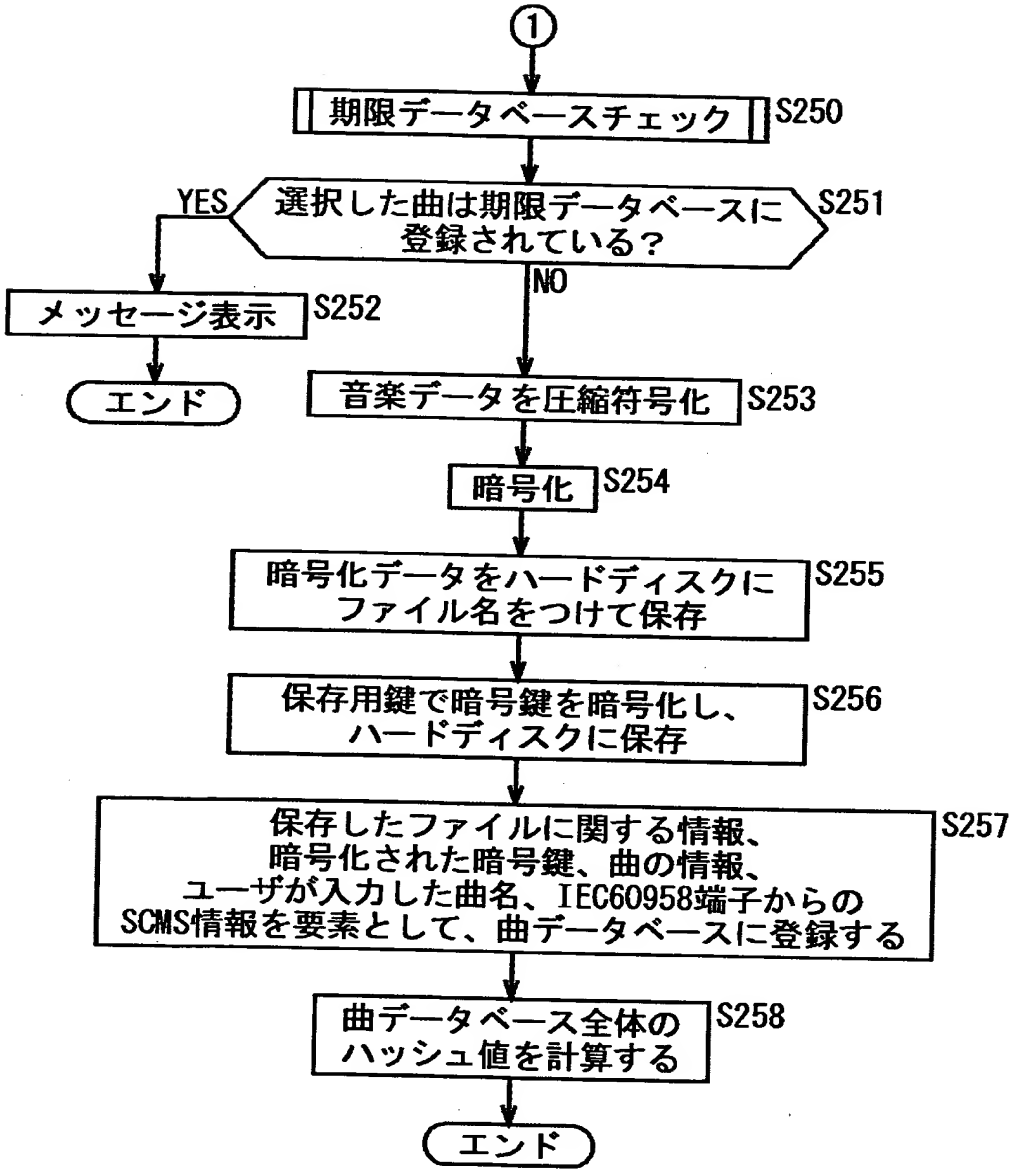
【図２０】



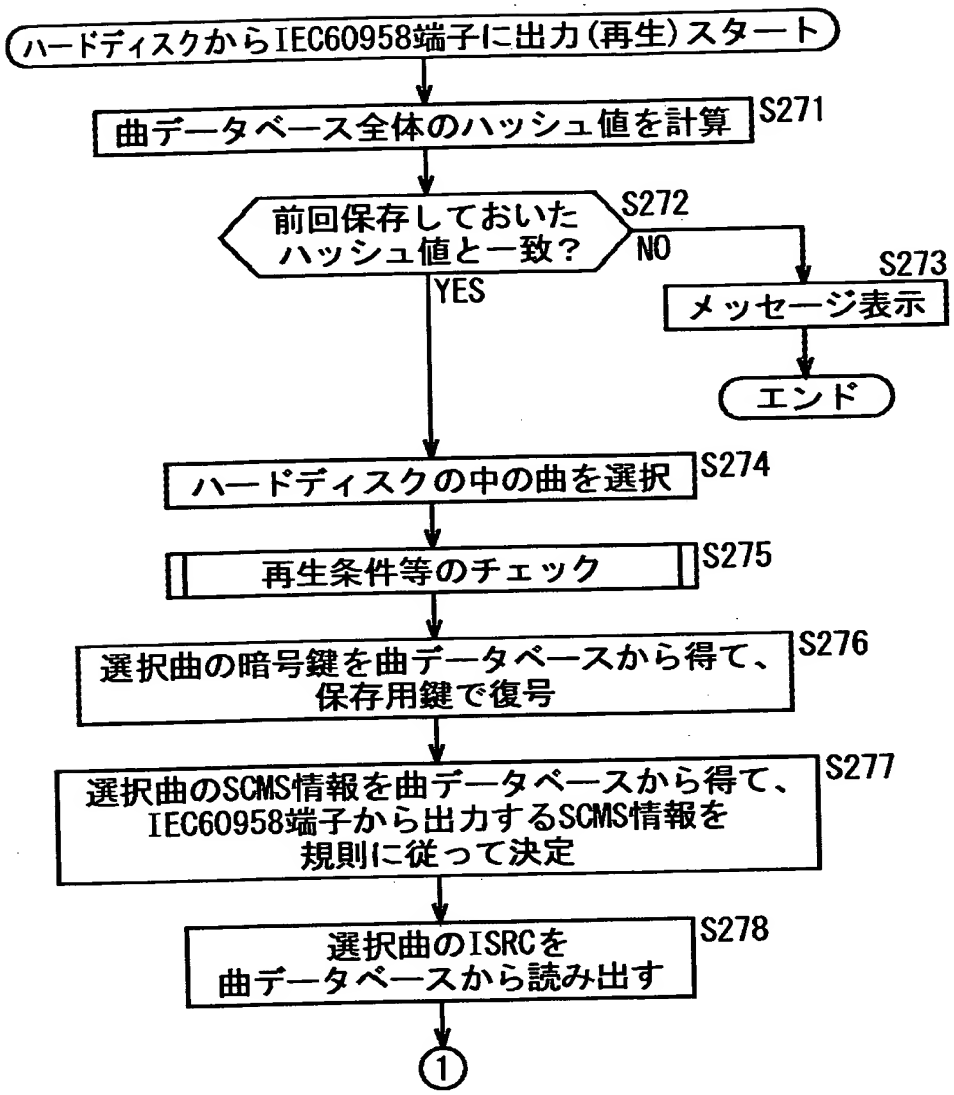
【図２１】


IEC60958端子からハードディスクへコピースタート
CDプレーヤのIEC60958出力端子を
PCのIEC60958入力端子に接続する
S241
録音する曲名をPCから入力
S242
CDプレーヤの再生開始指令
S243
CDプレーヤが再生出力する音楽データが、
IEC60958端子経由でPCに転送される
S244
PCは、IEC60958端子のデータから、
SCMSを読み取る
S245
S246
コピー禁止？
YES
NO
ウォータマーク読み出し
S248
S249
コピー禁止？
YES
NO
①
S247
メッセージ表示
エンド

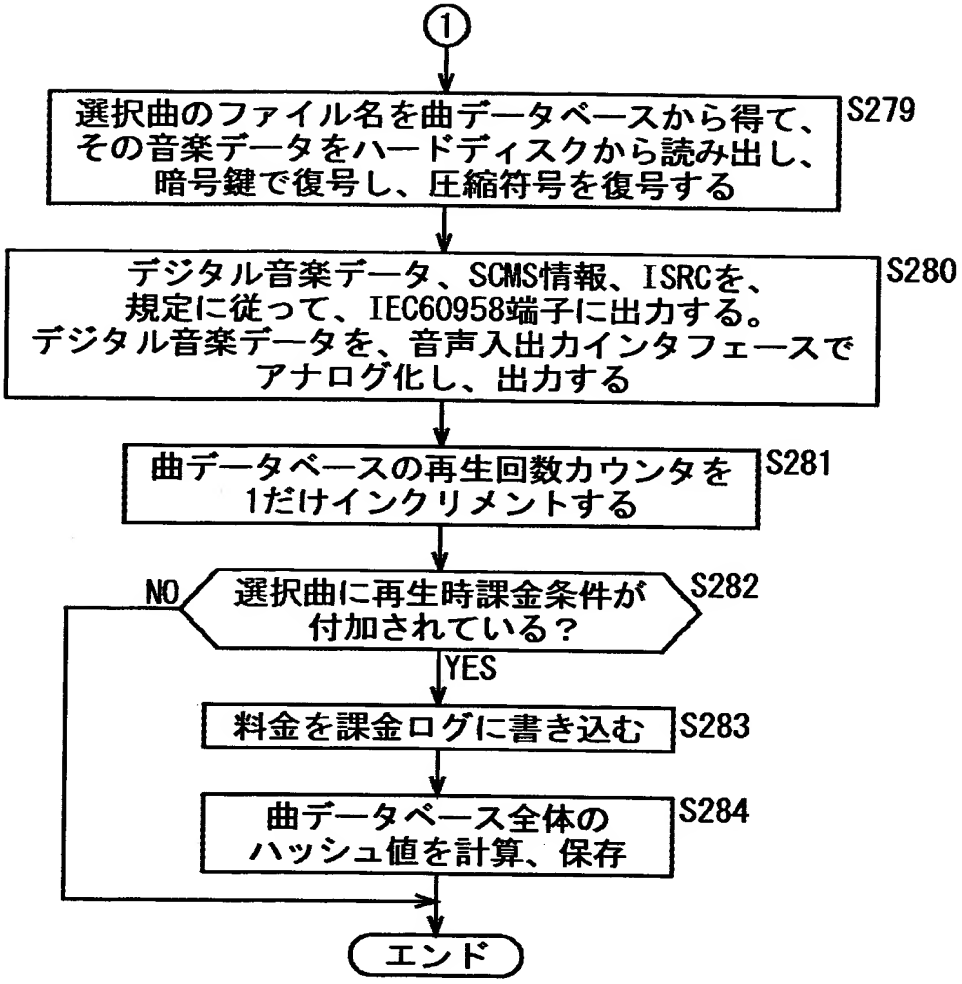
【図２２】


①
期限データベースチェック
S250
選択した曲は期限データベースに登録されている？
S251
YES
NO
メッセージ表示
S252
エンド
音楽データを圧縮符号化
S253
暗号化
S254
暗号化データをハードディスクにファイル名をつけて保存
S255
保存用鍵で暗号鍵を暗号化し、ハードディスクに保存
S256
保存したファイルに関する情報、暗号化された暗号鍵、曲の情報、ユーザが入力した曲名、IEC60958端子からのSCMS情報を要素として、曲データベースに登録する
S257
曲データベース全体のハッシュ値を計算する
S258
エンド

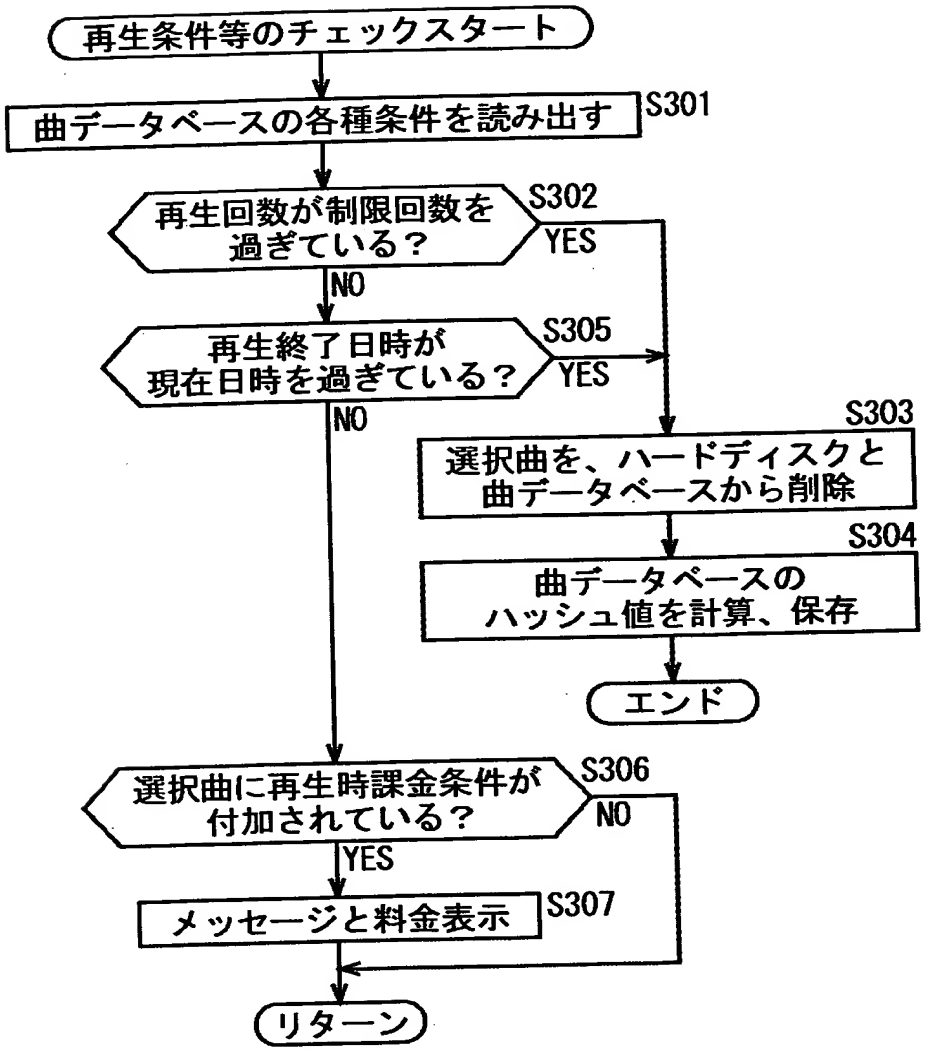
【図２３】


ハードディスクからIEC60958端子に出力(再生)スタート
曲データベース全体のハッシュ値を計算
S271
前回保存しておいた
ハッシュ値と一致？
S272
NO
YES
S273
メッセージ表示
エンド
ハードディスクの中の曲を選択
S274
再生条件等のチェック
S275
選択曲の暗号鍵を曲データベースから得て、
保存用鍵で復号
S276
選択曲のSCMS情報を曲データベースから得て、
IEC60958端子から出力するSCMS情報を
規則に従って決定
S277
選択曲のISRCを
曲データベースから読み出す
S278
①

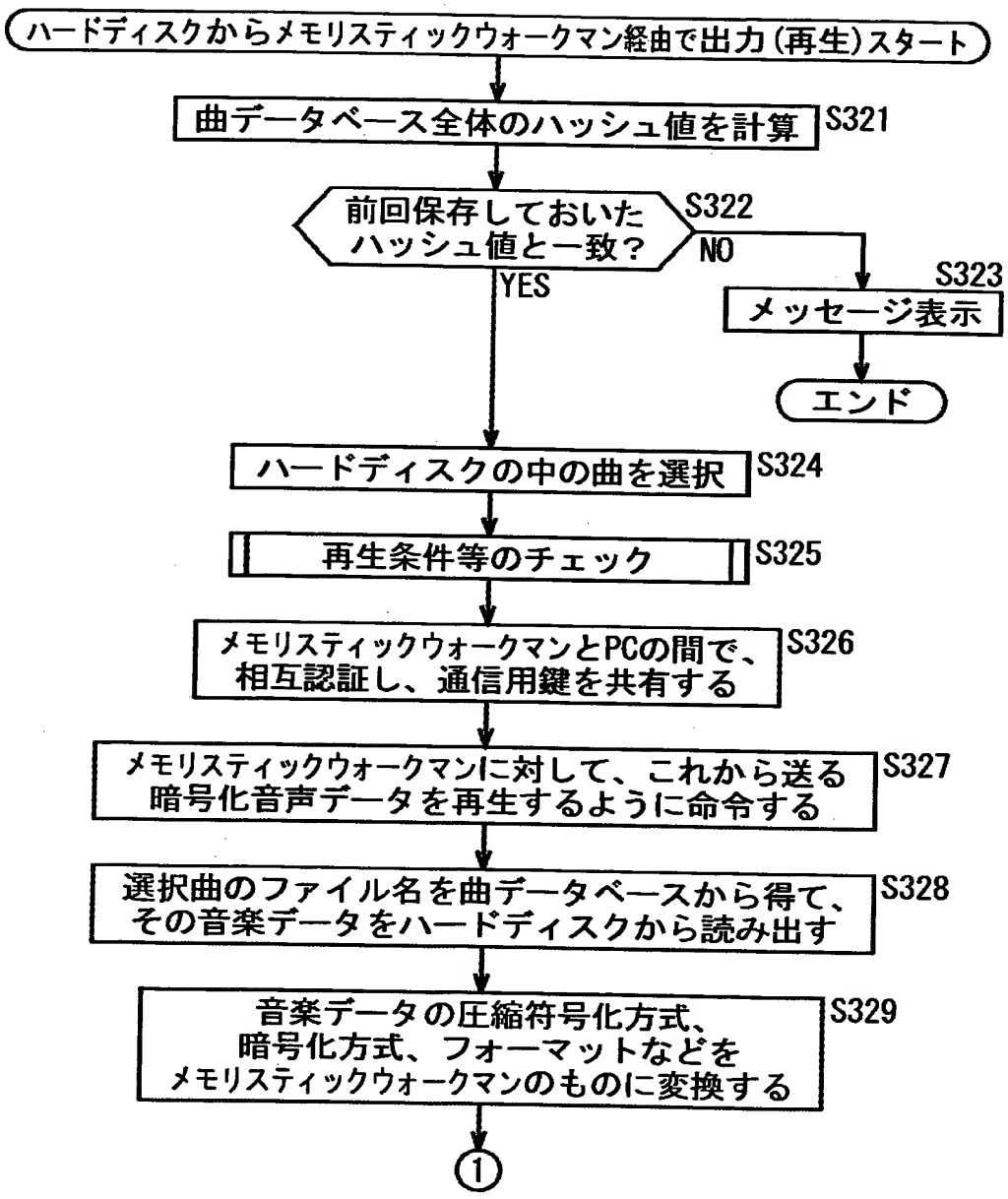
【図２４】


①
選択曲のファイル名を曲データベースから得て、その音楽データをハードディスクから読み出し、暗号鍵で復号し、圧縮符号を復号する
S279
デジタル音楽データ、SCMS情報、ISRCを、規定に従って、IEC60958端子に出力する。デジタル音楽データを、音声入出力インタフェースでアナログ化し、出力する
S280
曲データベースの再生回数カウンタを1だけインクリメントする
S281
NO
選択曲に再生時課金条件が付加されている？
S282
YES
料金を課金ログに書き込む
S283
曲データベース全体のハッシュ値を計算、保存
S284
エンド

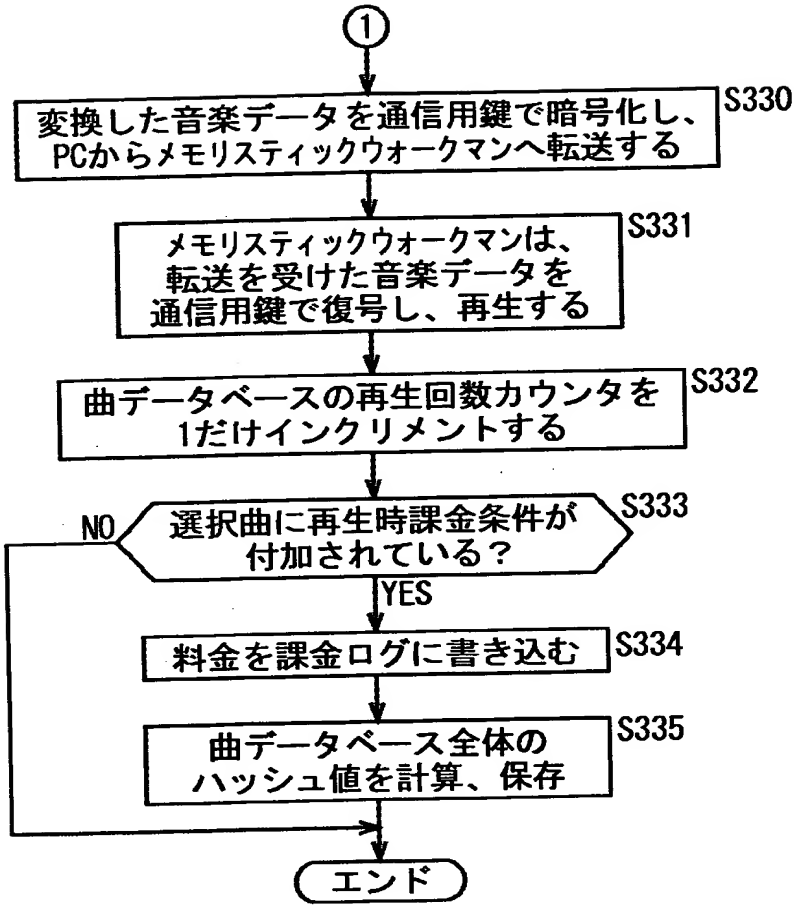
【図２５】


再生条件等のチェックスタート
曲データベースの各種条件を読み出す
S301
再生回数が制限回数を過ぎている？
S302
YES
NO
再生終了日時が現在日時を過ぎている？
S305
YES
NO
S303
選択曲を、ハードディスクと曲データベースから削除
S304
曲データベースのハッシュ値を計算、保存
エンド
選択曲に再生時課金条件が付加されている？
S306
NO
YES
メッセージと料金表示
S307
リターン

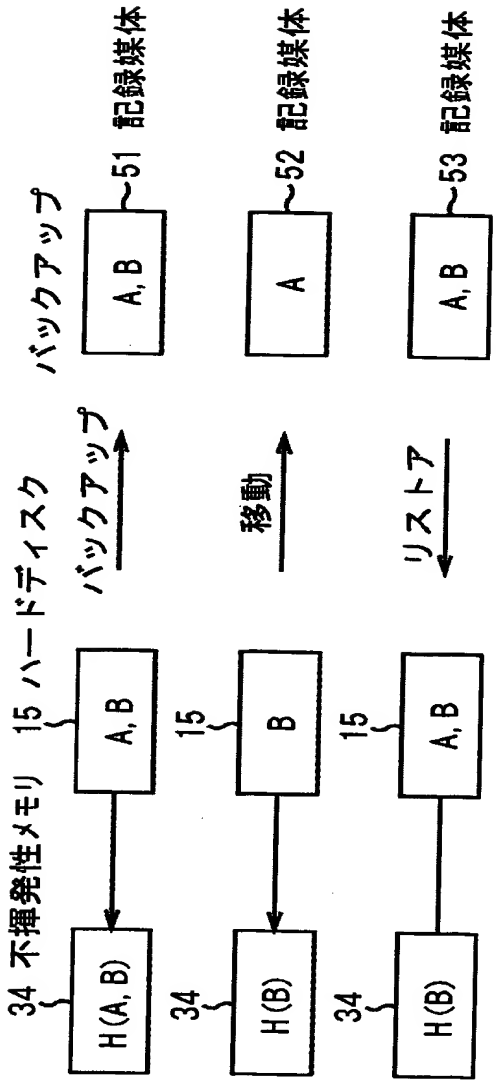
【図２６】


ハードディスクからメモリスティックウォークマン経由で出力(再生)スタート
曲データベース全体のハッシュ値を計算
S321
前回保存しておいた
ハッシュ値と一致？
S322
NO
YES
S323
メッセージ表示
エンド
ハードディスクの中の曲を選択
S324
再生条件等のチェック
S325
メモリスティックウォークマンとPCの間で、
相互認証し、通信用鍵を共有する
S326
メモリスティックウォークマンに対して、これから送る
暗号化音声データを再生するように命令する
S327
選択曲のファイル名を曲データベースから得て、
その音楽データをハードディスクから読み出す
S328
音楽データの圧縮符号化方式、
暗号化方式、フォーマットなどを
メモリスティックウォークマンのものに変換する
S329
①

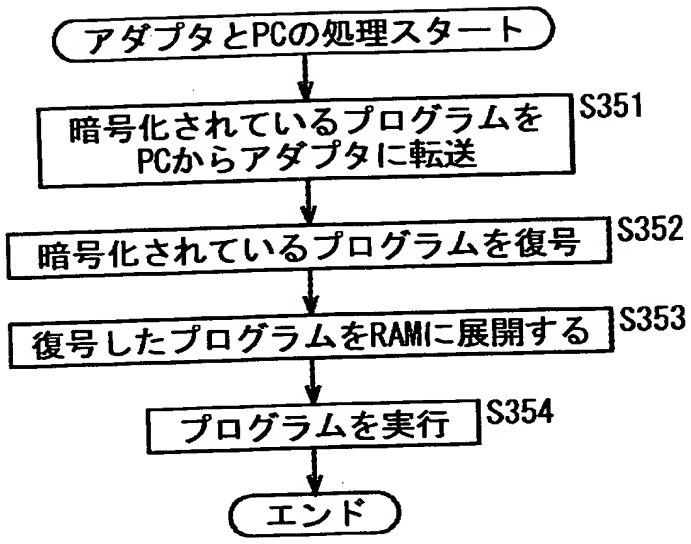
【図２７】


①
変換した音楽データを通信用鍵で暗号化し、PCからメモリスティックウォークマンへ転送する
S330
メモリスティックウォークマンは、転送を受けた音楽データを通信用鍵で復号し、再生する
S331
曲データベースの再生回数カウンタを1だけインクリメントする
S332
NO
選択曲に再生時課金条件が付加されている？
S333
YES
料金を課金ログに書き込む
S334
曲データベース全体のハッシュ値を計算、保存
S335
エンド

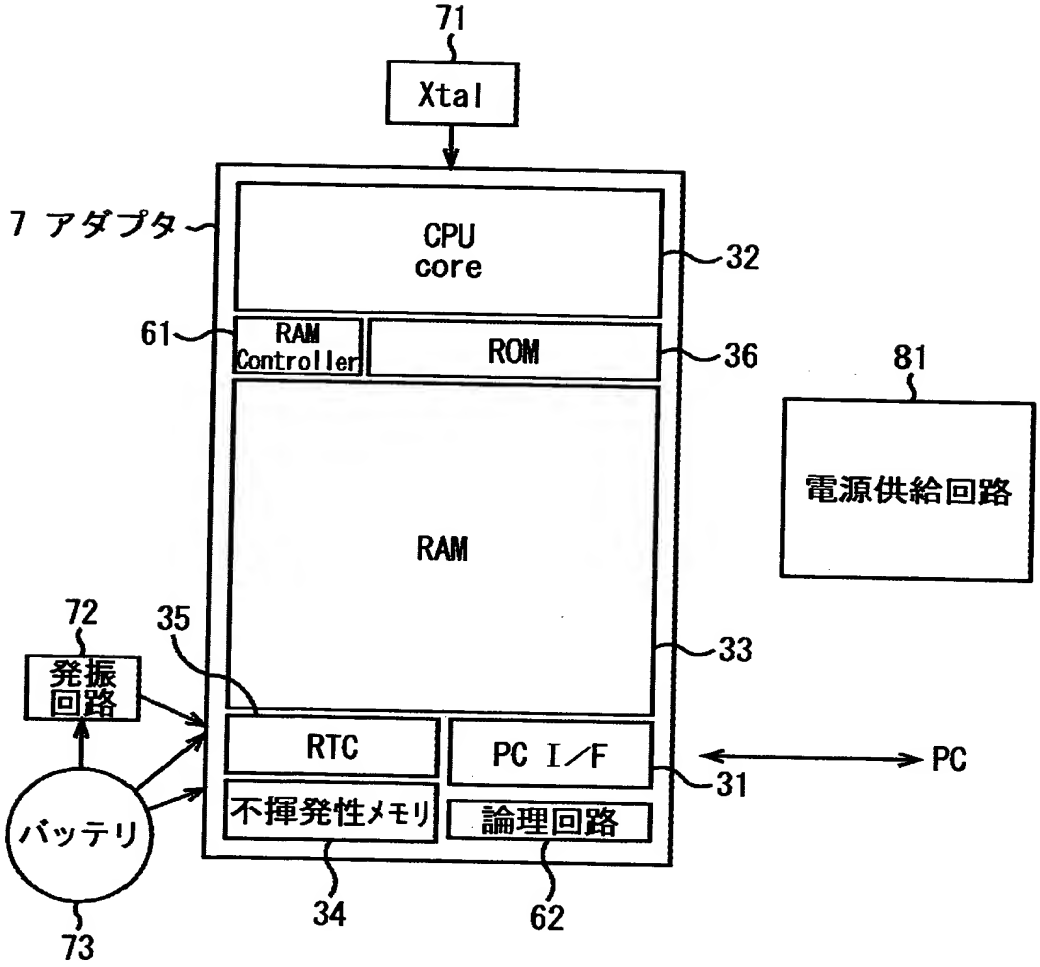
【図２８】


34 不揮発性メモリ
15 ハードディスク
バックアップ
移動
リストア
バックアップ
51 記録媒体
52 記録媒体
53 記録媒体
H(A, B)
H(B)
H(B)
A, B
B
A, B
A, B
A
A, B

【図２９】

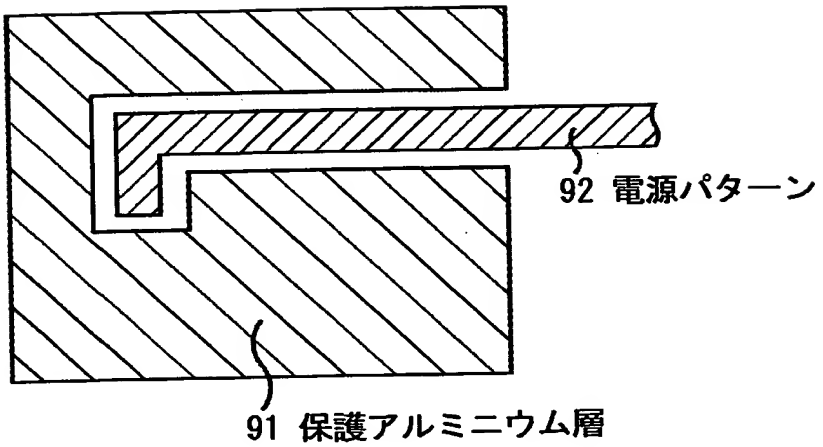

アダプタとPCの処理スタート
暗号化されているプログラムを
PCからアダプタに転送
S351
暗号化されているプログラムを復号
S352
復号したプログラムをRAMに展開する
S353
プログラムを実行
S354
エンド

【図３０】

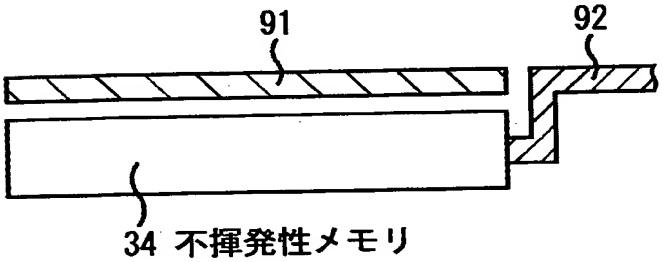

71
Xtal
7 アダプタ
CPU
core
32
61
RAM
Controller
ROM
36
81
電源供給回路
RAM
72
35
33
発振
回路
RTC
PC I／F
PC
31
バッテリ
不揮発性メモリ
論理回路
34
62
73

【図３１】

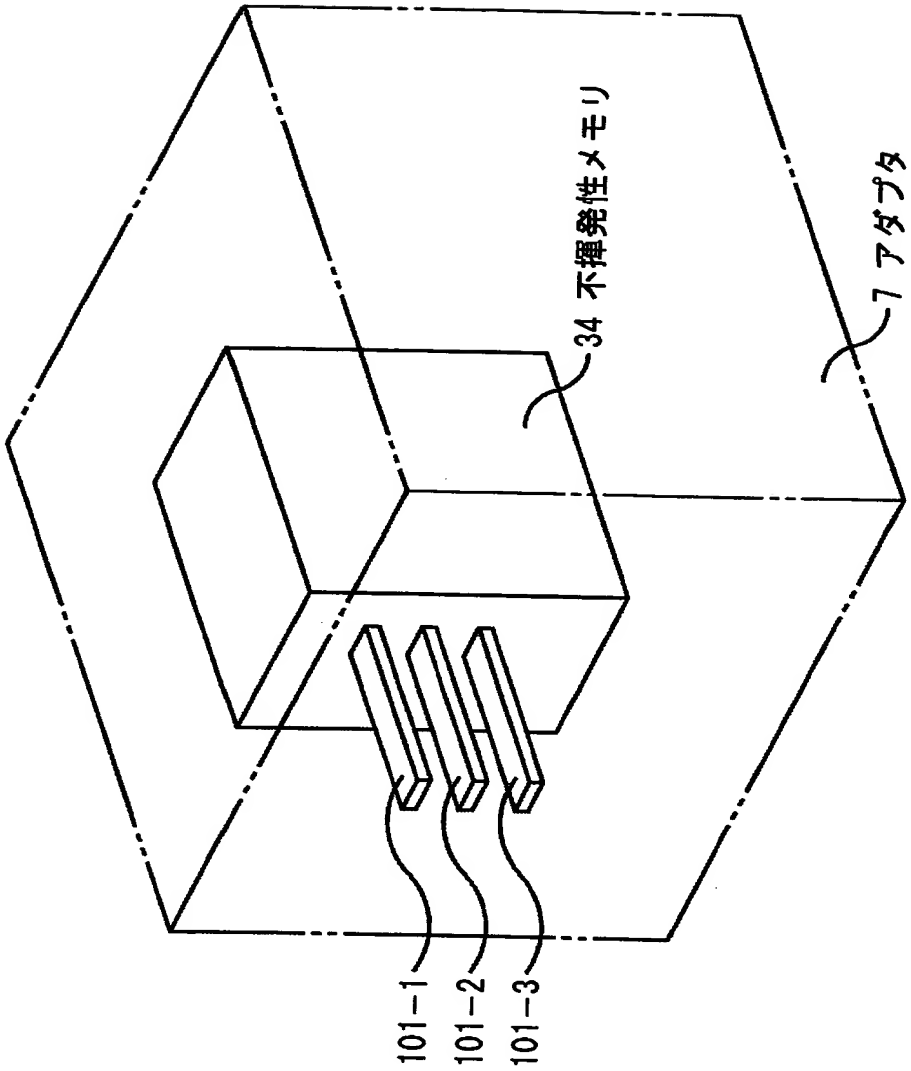
(A)



(B)

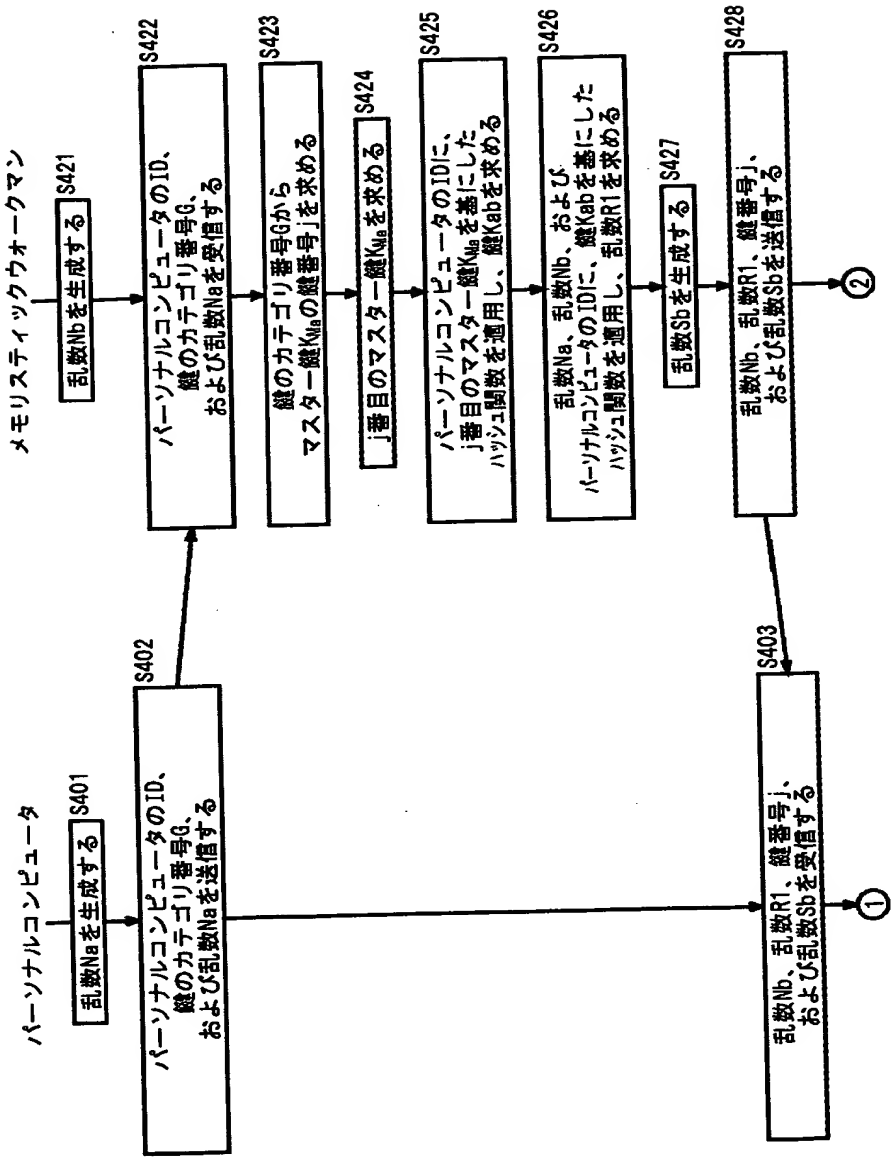


【図３２】



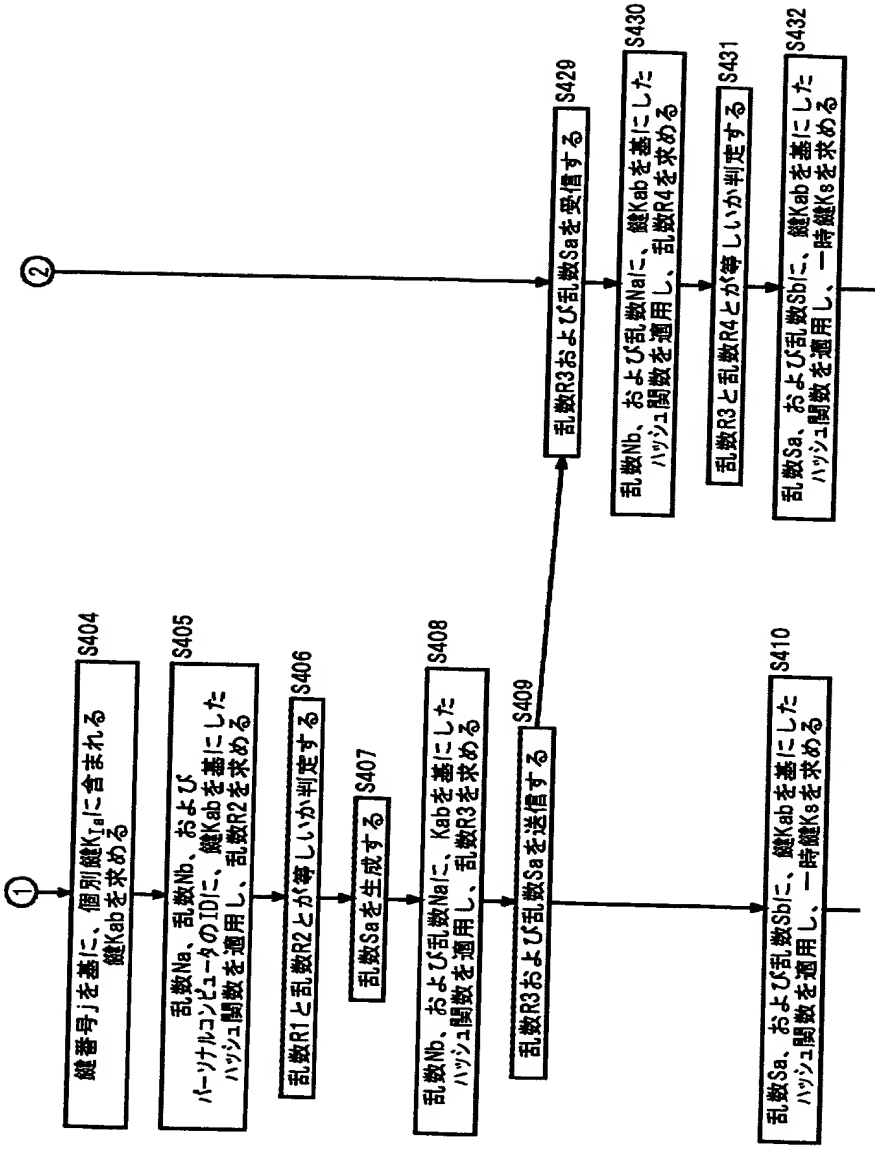
【図３３】

(33-1)


パーソナルコンピュータ
メモリスティックウォークマン
乱数Naを生成する
S401
乱数Nbを生成する
S421
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを送信する
S402
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを受信する
S422
鍵のカテゴリ番号Gから
マスター鍵K_{Na}の鍵番号jを求める
S423
j番目のマスター鍵K_{Na}を求める
S424
パーソナルコンピュータのIDに、
j番目のマスター鍵K_{Na}を基にした
ハッシュ関数を適用し、鍵Kabを求める
S425
乱数Na、乱数Nb、および
パーソナルコンピュータのIDに、鍵Kabを基にした
ハッシュ関数を適用し、乱数R1を求める
S426
乱数Sbを生成する
S427
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを送信する
S428
①
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを受信する
S403
②

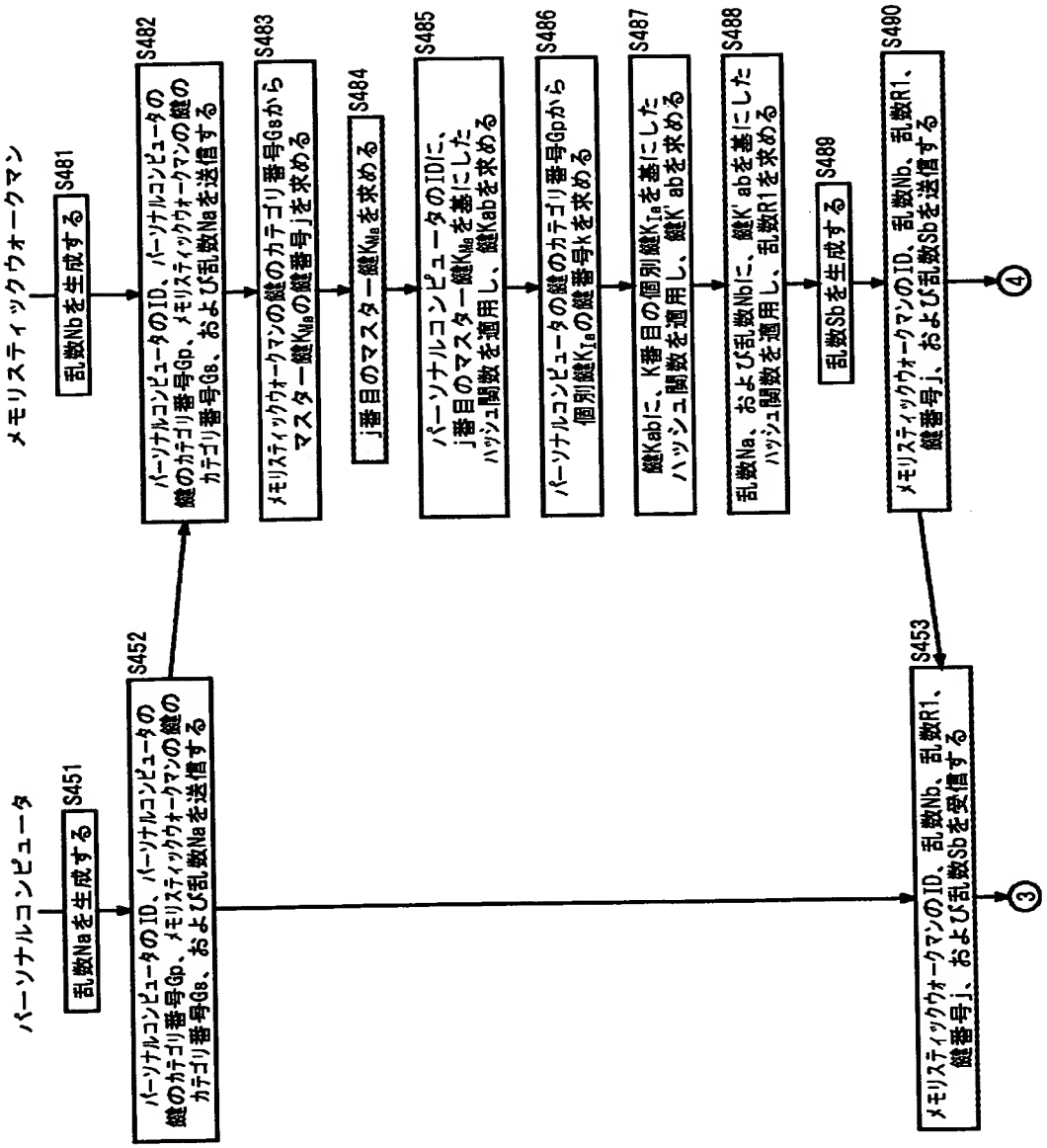
【図３４】

(33-2)


①
鍵番号jを基に、個別鍵K_{Ij}に含まれる鍵Kabを求める
S404
乱数Na、乱数Nb、およびパーソナルコンピュータのIDに、鍵Kabを基にしたハッシュ関数を適用し、乱数R2を求める
S405
乱数R1と乱数R2とが等しいか判定する
S406
乱数Saを生成する
S407
乱数Nb、およびに乱数Nalに、Kabを基にしたハッシュ関数を適用し、乱数R3を求める
S408
乱数R3およびに乱数Saを送信する
S409
乱数Sa、およびに乱数Sblに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S410
②
乱数R3およびに乱数Saを受信する
S429
乱数Nb、およびに乱数Nalに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S430
乱数R3と乱数R4とが等しいか判定する
S431
乱数Sa、およびに乱数Sblに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S432

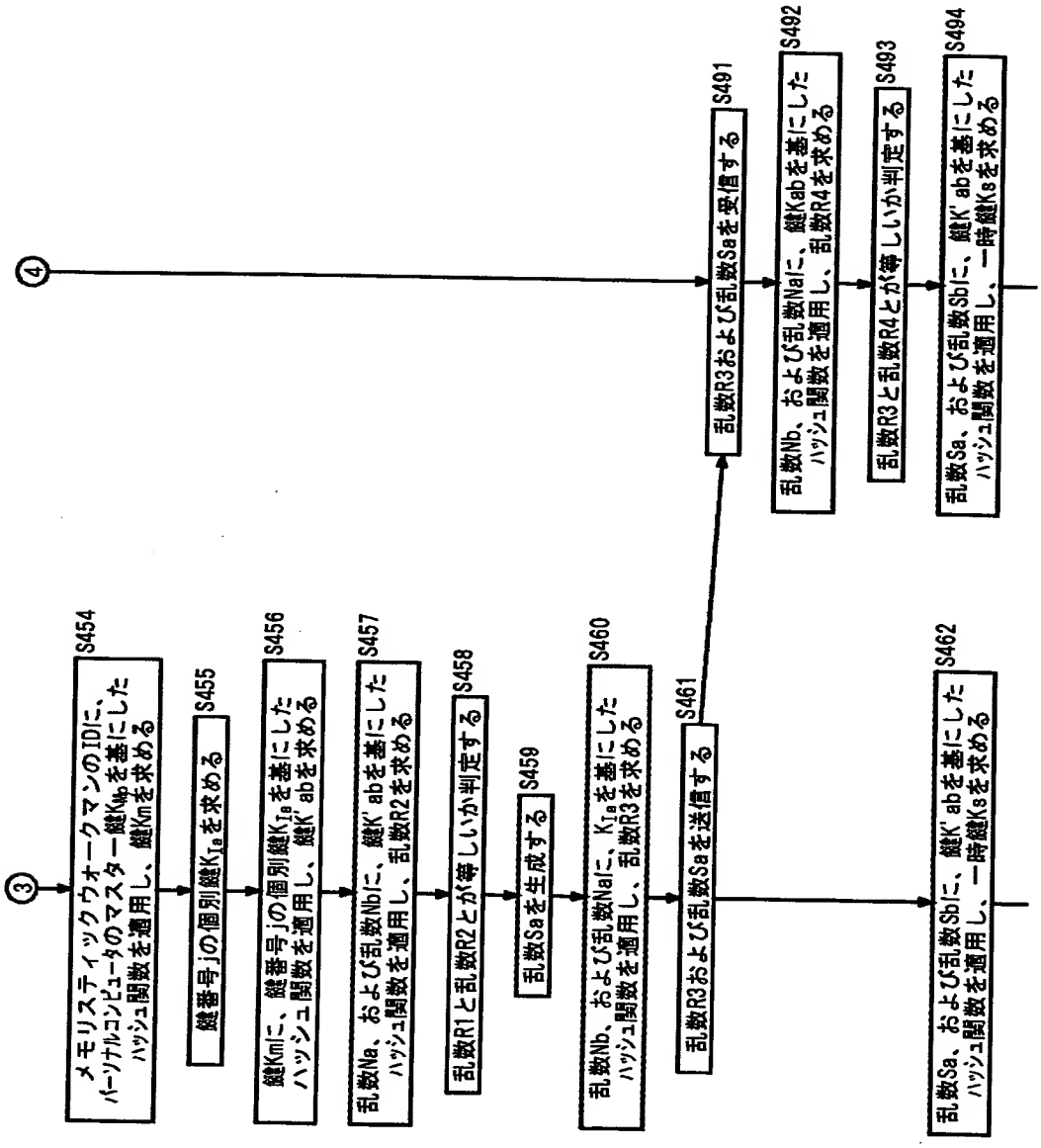
【図３５】

(35-1)

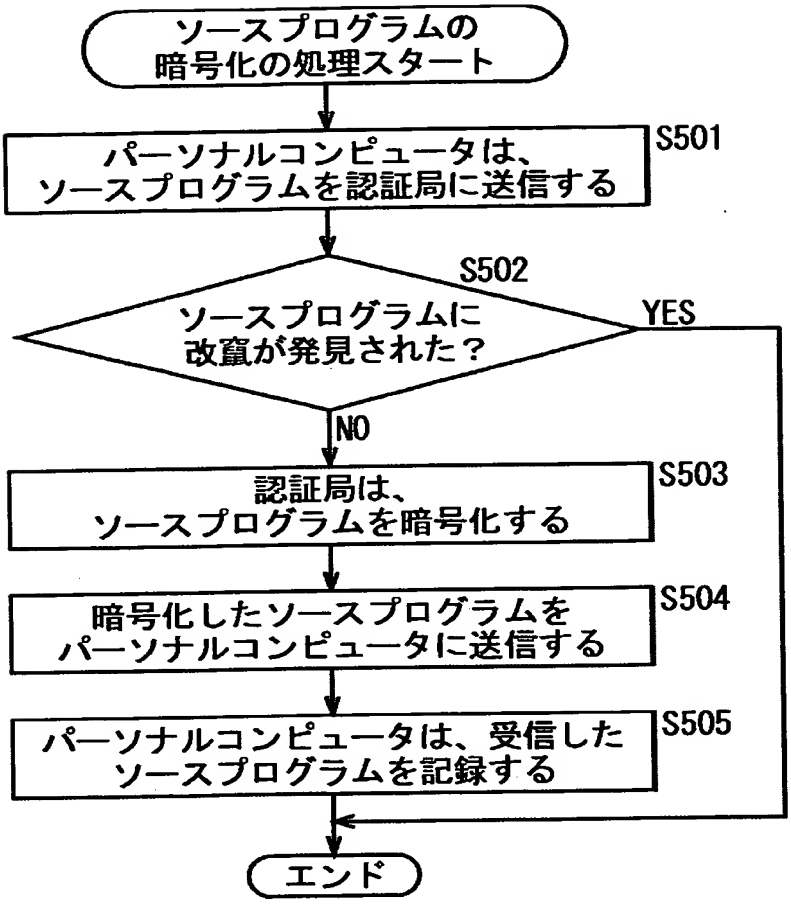

パーソナルコンピュータ
メモリスティックウォークマン
乱数Naを生成する
S451
乱数Nbを生成する
S481
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、メモリスティックウォークマンの鍵のカテゴリ番号Gs、および乱数Naを送信する
S452
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、メモリスティックウォークマンの鍵のカテゴリ番号Gs、および乱数Naを送信する
S482
メモリスティックウォークマンの鍵のカテゴリ番号Gsからマスター鍵K_{Ma}の鍵番号jを求める
S483
j番目のマスター鍵K_{Ma}を求める
S484
パーソナルコンピュータのIDに、j番目のマスター鍵K_{Ma}を基にしたハッシュ関数を適用し、鍵Kabを求める
S485
パーソナルコンピュータの鍵のカテゴリ番号Gpから個別鍵K_{Ia}の鍵番号kを求める
S486
鍵Kabに、K番目の個別鍵K_{Ia}を基にしたハッシュ関数を適用し、鍵K'abを求める
S487
乱数Na、および乱数Nbに、鍵K'abを基にしたハッシュ関数を適用し、乱数R1を求める
S488
乱数Sbを生成する
S489
メモリスティックウォークマンのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを送信する
S490
④
メモリスティックウォークマンのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを受信する
S453
③

【図３６】

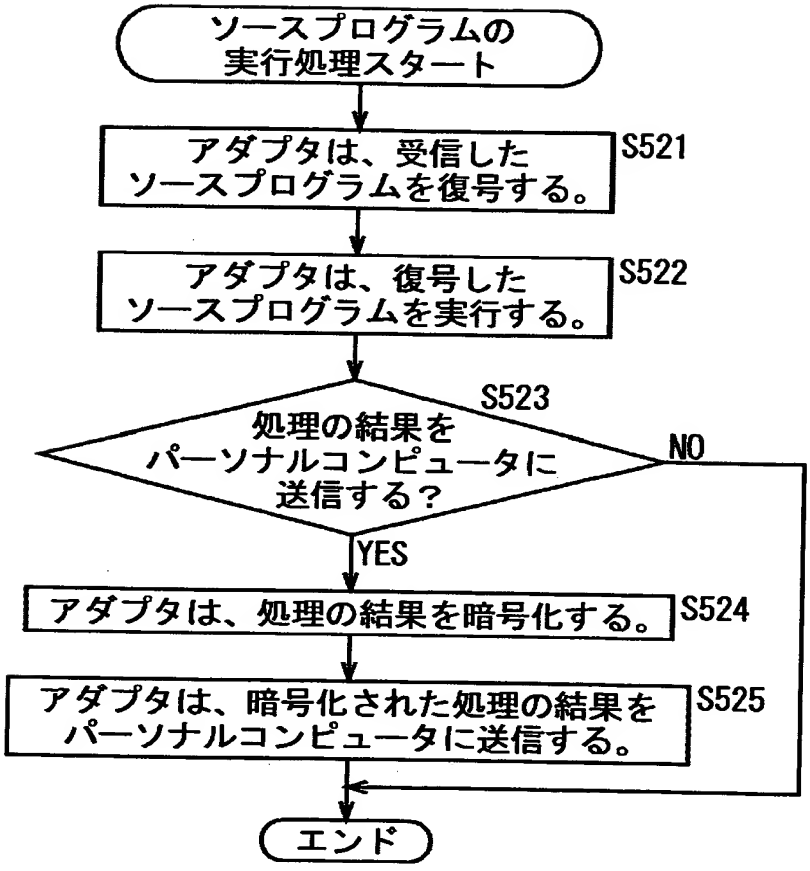
(35-2)


③
メモリスティックウォークマンのIDに、パーソナルコンピュータのマスター鍵K_{Mb}を基にしたハッシュ関数を適用し、鍵Kmを求める
S454
鍵番号jの個別鍵K_{Ia}を求める
S455
鍵Kmに、鍵番号jの個別鍵K_{Ia}を基にしたハッシュ関数を適用し、鍵K' abを求める
S456
乱数Na、および乱数Nbに、鍵K' abを基にしたハッシュ関数を適用し、乱数R2を求める
S457
乱数R1と乱数R2とが等しいか判定する
S458
乱数Saを生成する
S459
乱数Nb、および乱数Naに、K_{Ia}を基にしたハッシュ関数を適用し、乱数R3を求める
S460
乱数R3およびSaを送信する
S461
④
乱数R3およびSaを受信する
S491
乱数Nb、および乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S492
乱数R3と乱数R4とが等しいか判定する
S493
乱数Sa、および乱数Sbに、鍵K' abを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S494
乱数Sa、および乱数Sbに、鍵K' abを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S462

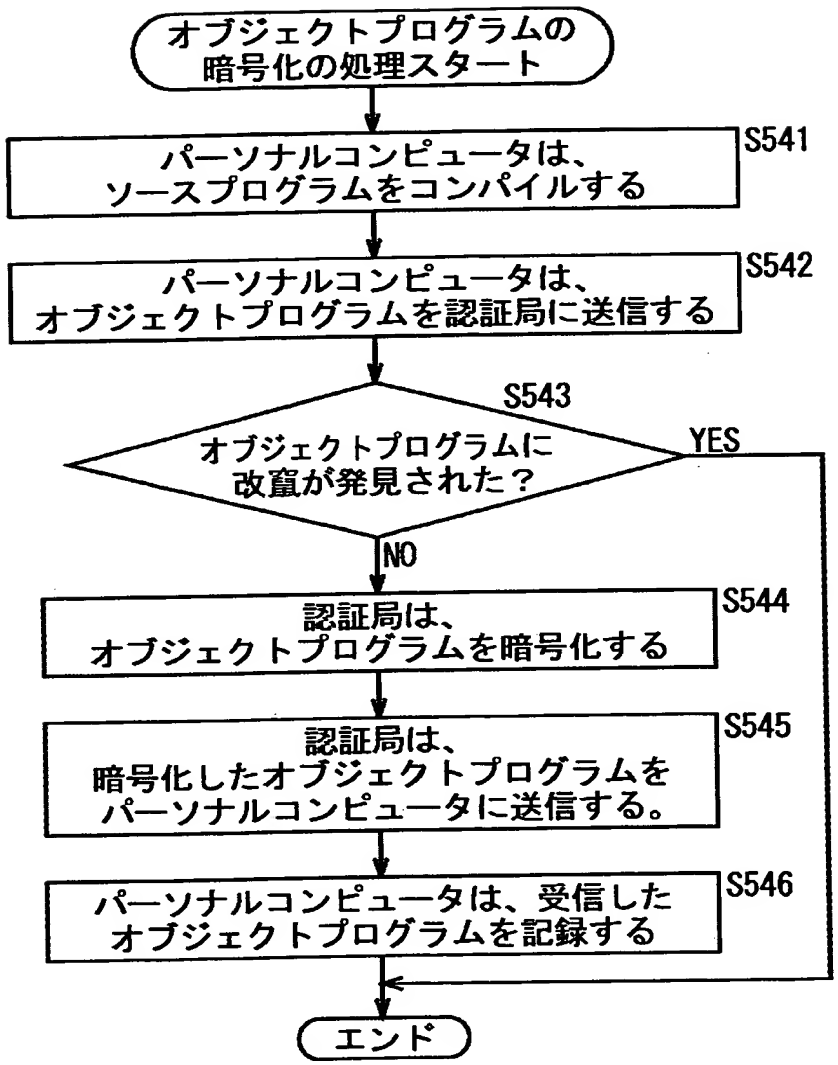
【図３７】


ソースプログラムの
暗号化の処理スタート
パーソナルコンピュータは、
ソースプログラムを認証局に送信する
S501
S502
ソースプログラムに
改竄が発見された？
YES
NO
認証局は、
ソースプログラムを暗号化する
S503
暗号化したソースプログラムを
パーソナルコンピュータに送信する
S504
パーソナルコンピュータは、受信した
ソースプログラムを記録する
S505
エンド

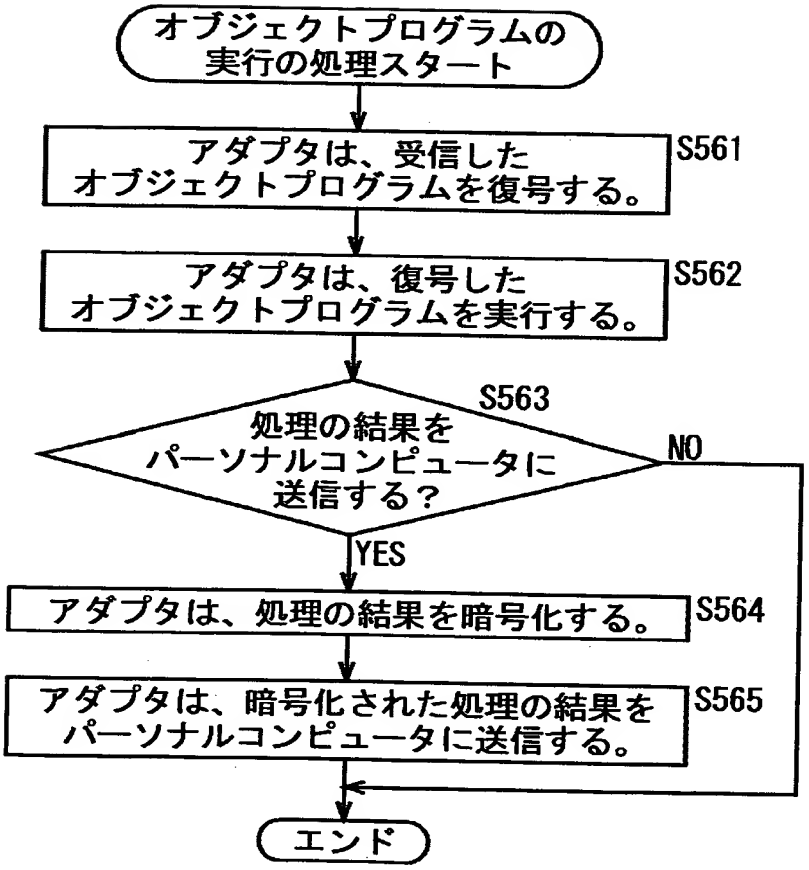
【図３８】


ソースプログラムの
実行処理スタート
アダプタは、受信した
ソースプログラムを復号する。
S521
アダプタは、復号した
ソースプログラムを実行する。
S522
S523
処理の結果を
パーソナルコンピュータに
送信する？
NO
YES
アダプタは、処理の結果を暗号化する。
S524
アダプタは、暗号化された処理の結果を
パーソナルコンピュータに送信する。
S525
エンド

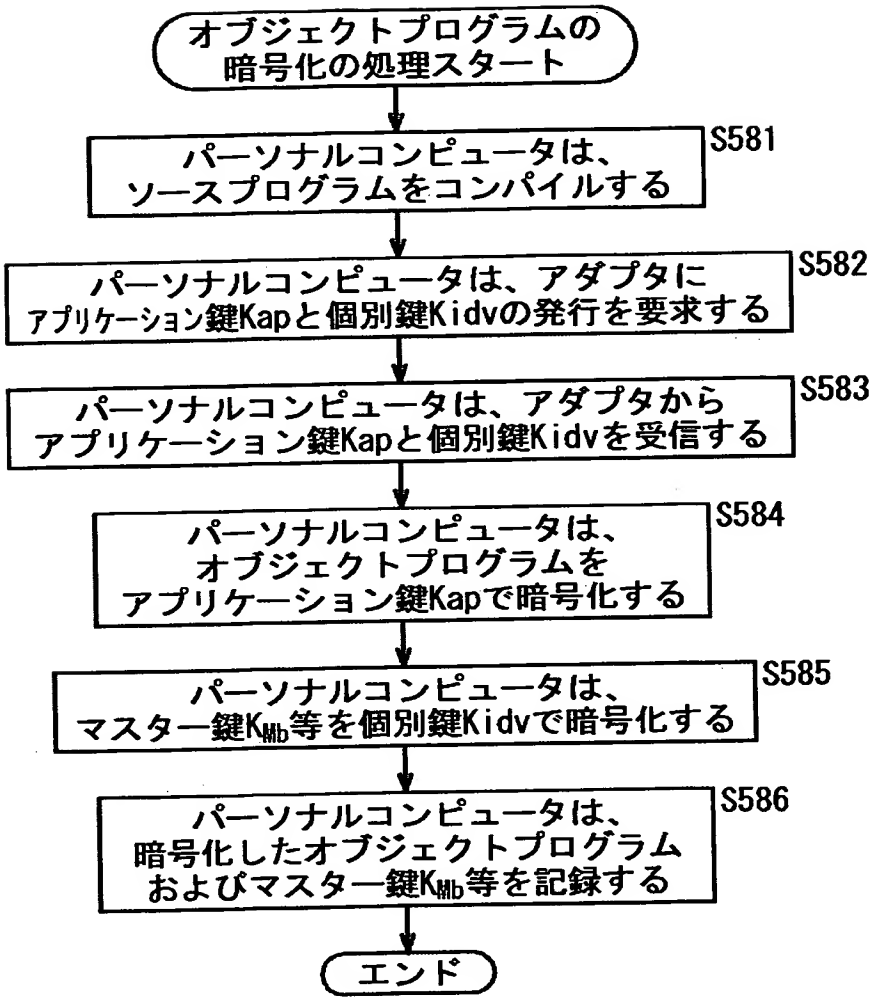
【図３９】


オブジェクトプログラムの
暗号化の処理スタート
パーソナルコンピュータは、
ソースプログラムをコンパイルする
S541
パーソナルコンピュータは、
オブジェクトプログラムを認証局に送信する
S542
S543
オブジェクトプログラムに
改竄が発見された？
YES
NO
認証局は、
オブジェクトプログラムを暗号化する
S544
認証局は、
暗号化したオブジェクトプログラムを
パーソナルコンピュータに送信する。
S545
パーソナルコンピュータは、受信した
オブジェクトプログラムを記録する
S546
エンド

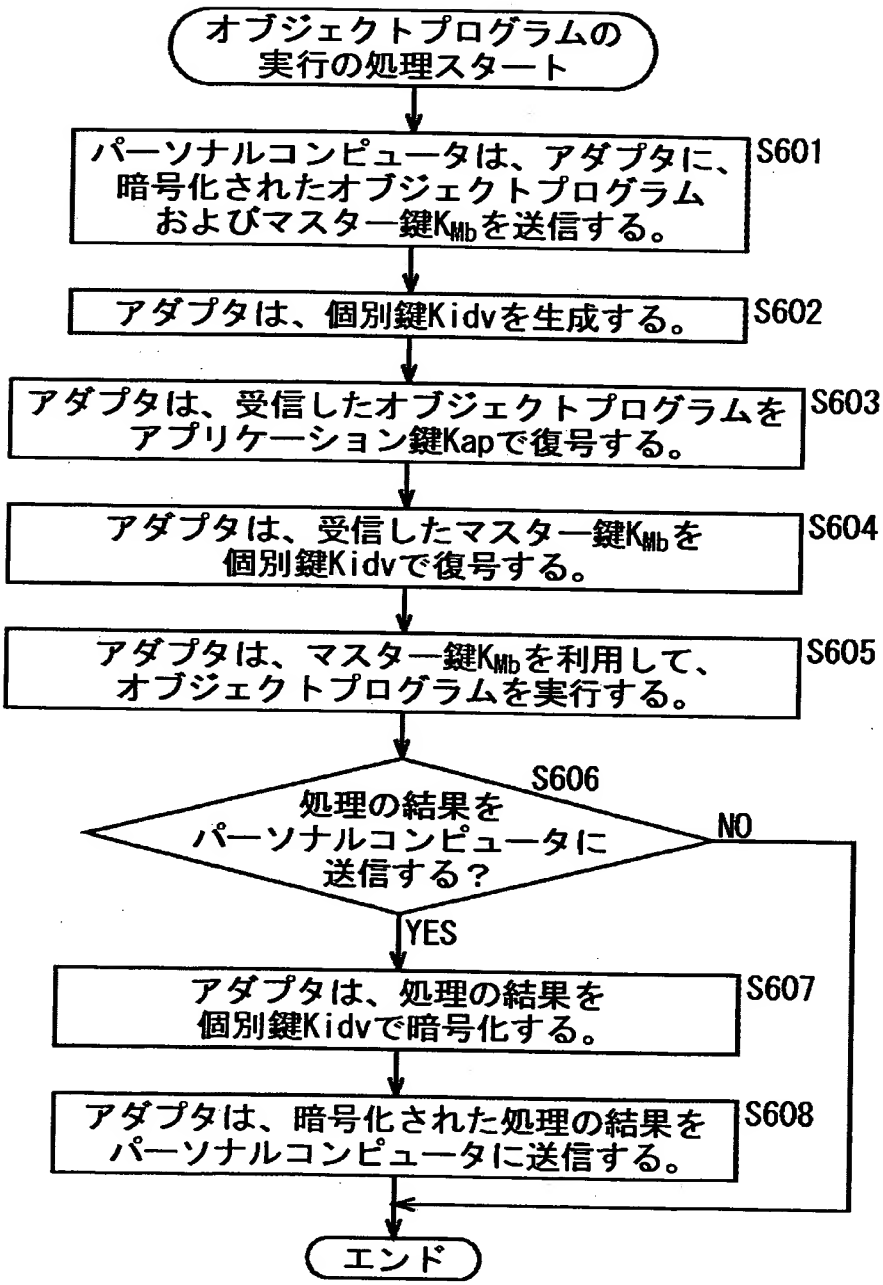
【図４０】


オブジェクトプログラムの
実行の処理スタート
アダプタは、受信した
オブジェクトプログラムを復号する。
S561
アダプタは、復号した
オブジェクトプログラムを実行する。
S562
S563
処理の結果を
パーソナルコンピュータに
送信する？
NO
YES
アダプタは、処理の結果を暗号化する。
S564
アダプタは、暗号化された処理の結果を
パーソナルコンピュータに送信する。
S565
エンド

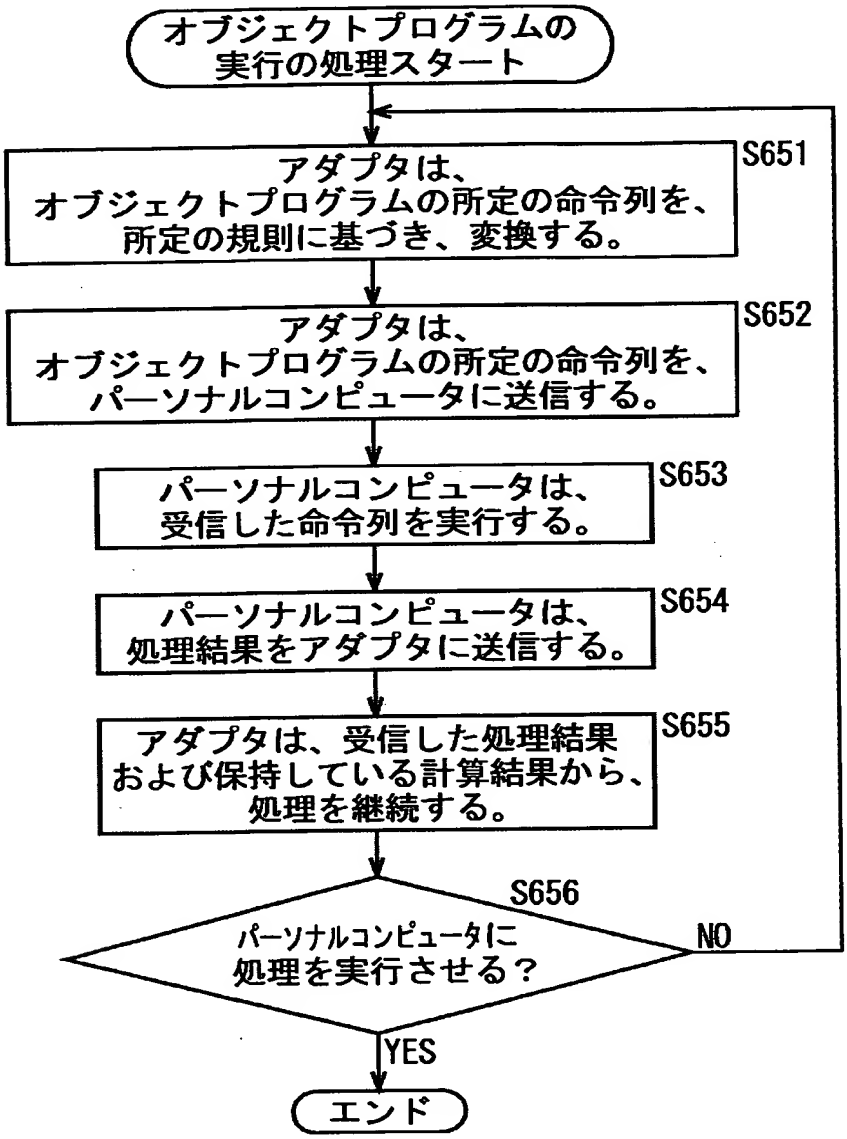
【図４１】


オブジェクトプログラムの
暗号化の処理スタート
パーソナルコンピュータは、
ソースプログラムをコンパイルする
S581
パーソナルコンピュータは、アダプタに
アプリケーション鍵Kapと個別鍵Kidvの発行を要求する
S582
パーソナルコンピュータは、アダプタから
アプリケーション鍵Kapと個別鍵Kidvを受信する
S583
パーソナルコンピュータは、
オブジェクトプログラムを
アプリケーション鍵Kapで暗号化する
S584
パーソナルコンピュータは、
マスター鍵K_{Mb}等を個別鍵Kidvで暗号化する
S585
パーソナルコンピュータは、
暗号化したオブジェクトプログラム
およびマスター鍵K_{Mb}等を記録する
S586
エンド

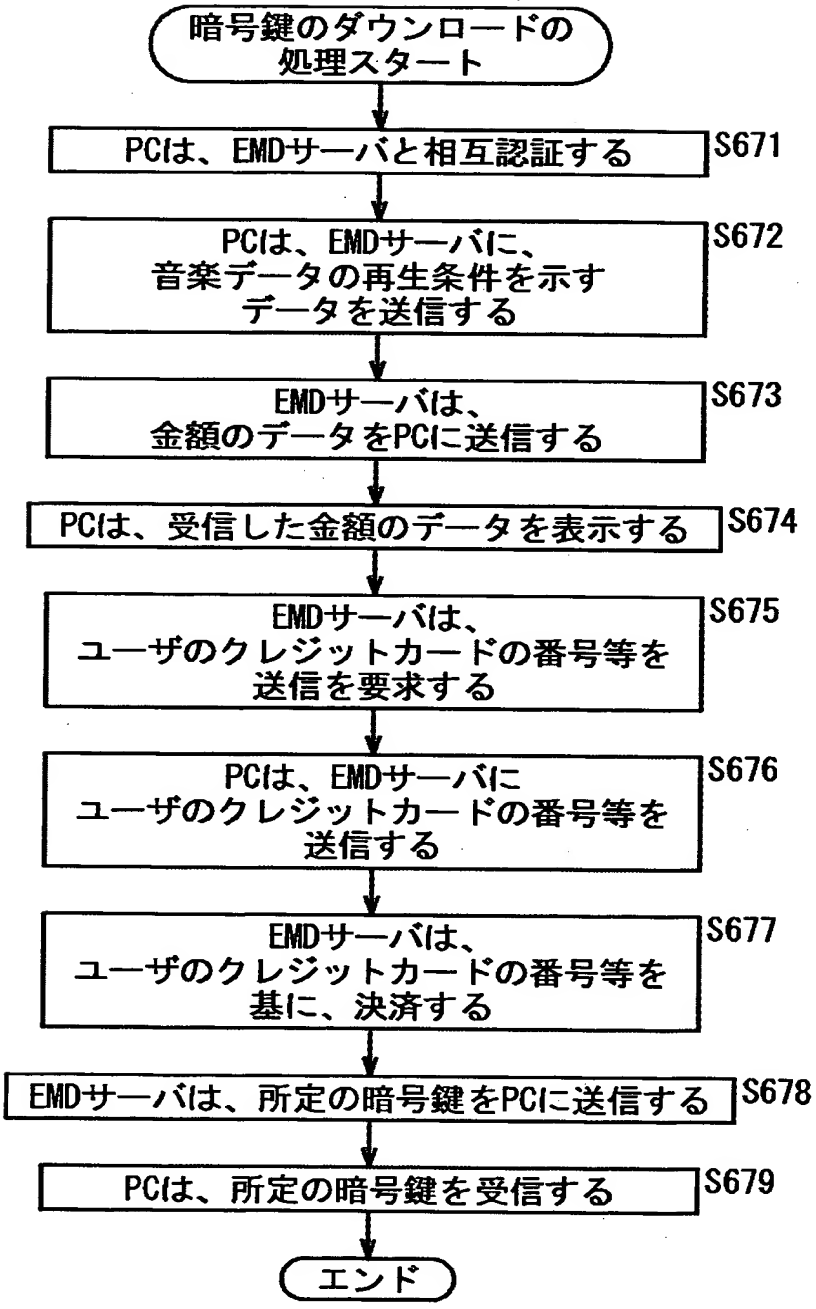
【図４２】


オブジェクトプログラムの実行の処理スタート
パーソナルコンピュータは、アダプタに、暗号化されたオブジェクトプログラムおよびマスター鍵K_{Mb}を送信する。
S601
アダプタは、個別鍵Kidvを生成する。
S602
アダプタは、受信したオブジェクトプログラムをアプリケーション鍵Kapで復号する。
S603
アダプタは、受信したマスター鍵K_{Mb}を個別鍵Kidvで復号する。
S604
アダプタは、マスター鍵K_{Mb}を利用して、オブジェクトプログラムを実行する。
S605
S606
処理の結果をパーソナルコンピュータに送信する？
NO
YES
アダプタは、処理の結果を個別鍵Kidvで暗号化する。
S607
アダプタは、暗号化された処理の結果をパーソナルコンピュータに送信する。
S608
エンド

【図４３】


オブジェクトプログラムの
実行の処理スタート
アダプタは、
オブジェクトプログラムの所定の命令列を、
所定の規則に基づき、変換する。
S651
アダプタは、
オブジェクトプログラムの所定の命令列を、
パーソナルコンピュータに送信する。
S652
パーソナルコンピュータは、
受信した命令列を実行する。
S653
パーソナルコンピュータは、
処理結果をアダプタに送信する。
S654
アダプタは、受信した処理結果
および保持している計算結果から、
処理を継続する。
S655
S656
パーソナルコンピュータに
処理を実行させる？
NO
YES
エンド

【図４４】


暗号鍵のダウンロードの処理スタート
PCは、EMDサーバと相互認証する
S671
PCは、EMDサーバに、音楽データの再生条件を示すデータを送信する
S672
EMDサーバは、金額のデータをPCに送信する
S673
PCは、受信した金額のデータを表示する
S674
EMDサーバは、ユーザのクレジットカードの番号等を送信を要求する
S675
PCは、EMDサーバにユーザのクレジットカードの番号等を送信する
S676
EMDサーバは、ユーザのクレジットカードの番号等を基に、決済する
S677
EMDサーバは、所定の暗号鍵をPCに送信する
S678
PCは、所定の暗号鍵を受信する
S679
エンド

【書類名】　要約書

【要約】

【課題】　記憶されているデータが不正に読み出され、解析されるのを防止する。

【解決手段】　インターネット接続インターフェース１１は、アダプタ７に実行させるプログラムを認証局に送信するとともに、認証局から暗号化されたプログラムを受信する。ハードディスク１５は、認証局から受信した、暗号化されたプログラムを記録する。インターフェース１７は、ハードディスク１５に記録されているプログラムを、アダプタ７に送信する。

【選択図】　図１

出願人履歴情報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社